NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

JOINT NETWORKING COMMAND AND CONTROL (C2) COMMUNICATIONS AMONG DISTRIBUTED OPERATIONS, JCAS, AND JOINT FIRES

by

John S. Bommer, Jr.

June 2007

Thesis Co-Advisors: Rex Buddenberg
Carl Oros

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Joint Networking Command and Control (C2) Communications among Distributed Operations, Jcas, and Joint Fires		**5. FUNDING NUMBERS**	
6. AUTHOR(S) John S. Bommer, Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Institute of Technology (AFIT), Wright Patterson AFB, OH Air Force Communications Agency (AFCA), Scott AFB, IL Marine Corps Tactical Systems Support Activity (MCTSSA), Camp Pendleton, CA		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis postulates that the implementation of Mobile Ad Hoc Networking (MANET), Mesh and IEEE 802.16 products can support a Distributed Operations (DO) platoon. Ground and Air assets will use MANET, Mesh and IEEE 802.16 products to network a tactically deployed DO platoon through communications of ground and air based components. These ground and air components will link in an IP-based network and demonstrate the real-time exchange of data. This analysis will focus on the integration of traditional airborne assets with those of a DO platoon. By connecting those Sense, Decide, and Act (SDA) facets into a networked based architecture, the thesis experiments demonstrate that emerging commercial off the shelf (COTS) technologies can further advance data exchange between Service Oriented Architectures (SOA) and enhance the ability to provide Joint Close Air Support (JCAS) to DO platoons in an environment where Air Force, Navy, and Army components are available for fire support.

This thesis focuses on the integration of ground and air nodes into a networked based architecture using emerging COTS MANET, Mesh, and IEEE 802.16 technologies to further advance data exchange between simulated ground and air units.

14. SUBJECT TERMS COTS, Mesh, 802.16, SDA, SOA, Distributed Operations, DO, Airborne Networking, WIMAX, WLAN, UHF, QOS, MANET, Redline, Tacticomp, Multi Mesh Router, peer to peer, point to multi-point, JCAS, Joint Fires			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

JOINT NETWORKING COMMAND AND CONTROL (C2) COMMUNICATIONS AMONG DISTRIBUTED OPERATIONS, JCAS, AND JOINT FIRES

John S. Bommer, Jr.
Major, United States Air Force
B.S., Tennessee State University, 1993
M.S., Colorado Technical University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL, AND COMMUNICATIONS (C3))**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2007**

Author: John S. Bommer, Jr.
Major, United States Air Force

Approved by: Rex Buddenberg
Advisor

Carl Oros
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis postulates that the implementation of Mobile Ad Hoc Networking (MANET), Mesh and IEEE 802.16 products can support a Distributed Operations (DO) platoon. Ground and Air assets will use MANET, Mesh and IEEE 802.16 products to network a tactically deployed DO platoon through communications of ground and air based components. These ground and air components will link in an IP-based network and demonstrate the real-time exchange of data. This analysis will focus on the integration of traditional airborne assets with those of a DO platoon. By connecting those Sense, Decide, and Act (SDA) facets into a networked based architecture, the thesis experiments demonstrate that emerging commercial off the shelf (COTS) technologies can further advance data exchange between Service Oriented Architectures (SOA) and enhance the ability to provide Joint Close Air Support (JCAS) to DO platoons in an environment where Air Force, Navy, and Army components are available for fire support.

This thesis focuses on the integration of ground and air nodes into a networked based architecture using emerging COTS MANET, Mesh, and IEEE 802.16 technologies to further advance data exchange between simulated ground and air units.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

> Nothing is so disgraceful as slovishness to custom; this is both ignorance and proof of it.
>
> De Saxe

I would like to thank God for continuing to bless me--His mercy endureth forever, and I must thank Him for providing Ezekiel 34: 28 & 30. I would also like to give special thanks to my ladies, Wilma, Morgan, and Colby. Without you, my accomplishments would mean nothing. In addition, I would like to thank my Father, Mother, Sisters, and Cousin for their encouragement and strength. Next, I would like to thank my Omega brothers, D.M.W. and M.F., friends, and classmates who made it easier for me to be away from family and still feel loved and supported. Also, I would like to thank Lt Col. Pfeiffer for giving me sight of the goal line. Last, but not least, I would like to thank my Thesis advisors for making me stronger.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

During OPERATION ENDURING FREEDOM (OEF) AND OPERATION IRAQI FREEDOM (OIF), the Marine Corps' maneuver warfare philosophy was solidified with maximum decentralization of decision-making, which was mainly guided by commander's intent. The concept of Distributed Operations (DO) is the deliberate use of networked capabilities to decentralize decision-making, so small units can locate, close with, and destroy asymmetric threats (Tovar, 2005). Small units are not expected to conduct traditional military operations, but they are expected to do more dynamic missions that execute in a disaggregated fashion. These units will be dispersed beyond the normal range of mutually supporting organic direct fires, but linked through a command and control (C2). According to the Institute for National Strategic Studies, National Defense University, C2 acts as procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (Snyder, 1993). With the linking of DO unit to C2 network by IP-enabled tools, the commander and DO unit will have a shared situational awareness. This shared situational awareness should enhance the commander's ability to act on real-time knowledge, coordinate with other Service commanders for interdependent, tactical and strategic actions, and enable increased access to Joint service support to the beyond line of site (BLOS) DO unit.

The Marine Corps is in the process of developing the DO concept into future warfighting capabilities that still focus on the Marine Corps core competencies of maneuver warfare. Marine Corps Warfighting Lab (MCWL) is currently conducting experiments that test current capabilities and develop future requirements for DO. In accordance with Joint Vision 2020, the Air Force has a C4ISR Flight Plan that conceptually links the Air Force C2 Constellation to the Marine Corps through FORCEnet. By enabling interoperability between the service architectures, the Joint C2 infrastructure will be improved by network-

enabled capabilities that could improve Joint Close Air Support (JCAS) or Joint Fires. JCAS is an element of Joint Fire support. It assists land, maritime, amphibious, and special operations forces (SOF) to move, maneuver, and control territory, populations, and key waters (JP 3-09.3, 2003). JCAS plays a critical role in our ability to engage, disrupt, and destroy an enemy. Joint Fires occurs when two or more services use lethal and non-lethal weapons in coordinated action toward a common goal (JP 3-09.3, 2003). By improving the possibility for our ground units to connect air units through the DO concept, our improved, network-enabled DO capabilities will shorten the kill chain, provide decision superiority due to better situational awareness provided by the forward deployed unit, and enhance the Joint Fires support provided by the Air Force, Navy and Army in a Network Centric Warfare (NCW) environment. NCW is defined as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization (Alberts, Garstka, and Stein, 2000). The DO concept is not about a supreme commander receiving inputs from battlespace sensors and fighting remotely. Warriors on the ground, the small infantry units, are prime discriminators, deciders, and actors (Tovar, 2005). Although this differs from NCW and USAF doctrine, there is still a lot of room for the DO concept to fuse with NCW doctrine and become a link between USMC and Joint service components. Joint-service and coalition operations, such as CAS, require shared approaches and technologies (Navy League of US, 2007). The following chapters will describe some charted courses for further exploration to bridge the divide in approaches and technologies.

B. OBJECTIVES

This thesis discusses the Joint Networking C2 architecture proposed to support Marines, Air Force, Navy, and Army in a Joint environment and provides an analysis of possible network infrastructure, technologies, and employment for

JCAS and Joint Fires support. In addition, this analysis will focus on the integration of traditional Service Oriented Architectures (SOAs) into a networked based architecture using emerging COTS technologies. SOA is an overall grouping of information services. These services involve communicating through the exchange of data elements, or could include two or more services coordinating to orchestrate an event or plan (Service-architecture.com, 2007). By improving SOA integration, the military can enhance our ability to achieve a networked communications environment to enhance Joint service capabilities by removing the demarcation-lines between communication infrastructures.

C. RESEARCH QUESTIONS

- Can a Joint C2 architecture using COTS equipment demonstrate communication with an air component and exchanging data between aerial vehicles and a DO platoon?
- Can IEEE 802.16, Mesh, and MANET technology establish a wireless backbone network architecture between DO platoons and connected UAVs to extend DO platoons capability to communicate with a Tactical Operation Center over 5 Kilometers beyond line of sight (BLOS)?
- What are the security considerations for ground, air, and near-space assets connected in a Joint Netcentric environment through COTS equipment?
- What specific equipment set would air nodes and a DO unit need to employ and successfully execute a mission and exchange of data?

D. SCOPE OF THESIS

Distributive Operations require by nature the integration of intelligence and communications. Marines need to communicate, collaborate and share a common picture, composed of voice and data as well as imagery, at all echelons. The forward deployed Marine will not only need to exchange data between the squads, but he will also need to exchange data with the airborne support nodes, Tactical Operations Centers, and other service components—if the situation necessitates.

My research will parallel efforts by NPS associates who are researching wireless networks, and it will attempt to demonstrate how to feasibly integrate products that comply with the IEEE 802.16 standard into these types of networks. Mesh is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by hopping from node to node until the destination is reached (Wikipedia, 2007). MANET is a network consisting of mobile routers with wireless network interfaces. Each node can function both as an end-host, but also as an intermediate router for other nodes in the network. The mobility of the nodes makes the network topology dynamic (Hafslund, Tonnesen, Rotvik, Andersson, and Kure; 2004). In addition, IEEE 802.16 is an IEEE standard for broadband wireless access aimed to provide high data rates over wide geographic areas. Also, WiMAX is the industry association associated with IEEE 802.16. By using these products that comply with the IEEE 802.16 standard, the thesis postulates that current technologies can enhance the DO methods of employment and allow for a practical transition to newer technology. In addition, the thesis analyzes new technology that can facilitate integrated IP data transfer between networked ground, air, and near-space assets. Last, the thesis discusses field tests of specific technologies, determines the capabilities, limitations, and lists further needed study for such equipment and its feasibility within DO, JCAS, and Joint Fires concept of operations. In field-testing these technologies, the experiment should provide observations of key areas of performance such as: integration; range; power consumption; data throughput; scalability; data security/authenticity; and method of employment. This thesis will provide an analysis of the equipment tested and detailed summary of observations. This analysis will be submitted to the Marine Corps Warfighting Lab (MCWL), Air Force Institute of Technology, and the Air Force Communications Agency.

E. METHODOLOGY

I used an established academic experiment methodology. I followed an AB-AB qualitative-type testing. Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) will be addressed in the experiment and equipment overview.

F. ORGANIZATION OF THESIS

- Background
  - Chapter I: Introduction
- High Level Conceptual Overview
  - Chapter II: Distributed Operations and Joint Fires C2
  - Chapter III: Domain Integration
- Technology Overview
  - Chapter IV: Layer Modularity
  - Chapter V: MAC to MAC Comparison
  - Chapter VI: MANET
  - Chapter VII: Mesh
- Demonstrated Experiments and Analysis
  - Chapter VIII: Experiment and Equipment Overview
- Conclusion and Future Experimentation
  - Chapter IX: Conclusion and Recommendation

THIS PAGE INTENTIONALLY LEFT BLANK

II. DISTRIBUTED OPERATIONS AND JOINT FIRES

A. INTRODUCTION

To allow DO units to carry out their mission and get Joint Fires support, the connectivity between ground elements and air nodes must be seamless and self-forming. The DO units, Navy, Army, and Air Force end nodes must have the means to communicate with each other and with the Land Forces Operating Center (LFOC), Supporting Arm Coordination Center (SACC), Marine Air Ground Task Force (MAGTAF) and Combat Air Operations Center (CAOC) from the edge of our combat environment. LFOC is the coordination center for the land forces engaged in the battlepsace. The SACC is the coordination center that helps to manage artillery or JCAS activity in support of ground forces. MAGTAF is the self-contained USMC deployment arm that manages its air and ground assets in the AOR. In addition, the CAOC is the coordination center for the air campaign and acts as the planning arm for the Joint Forces Air Component Commander (JFACC).

To provide a means of communication between these centers and edge units, the C2 network must be interoperable. Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services to enable them to operate effectively together (JP 1-02). Interoperability is an achievable goal that should be approached principally through system integration. Fighters (ships, battalions, and platoons) forming a network to take out pop-up targets would need a different technology (Tovar, 2005) other than our current means of point-to-point communications with LOS HF or UHF digital radios. Through the implementation of Mesh, MANET, and 802.16 technologies to bridge different SOAs, the Joint employment concept would demonstrate that data (voice, images, and text) could be transported from DO nodes to Air Force, Army, and Navy back to the DO nodes—in real-time. In this real-time Network Centric Warfare (NCW) environment, small distributed units will no longer be expected to only conduct

traditional military operations but act as more dynamic sensor units that execute in a disaggregated fashion dispersed beyond the normal range of mutually supporting organic direct fires, but linked through a C2 network. The intent of DO is not to replace traditional capabilities but rather enhance them to help shape battlespace. To help shape and extend the DO Battlespace, MCDP 1 states that in order to minimize research and development costs and fielding time, the Marine Corps will exploit existing capabilities—"off-the-shelf" technology—to the greatest extent possible. In that same vein of thought, AF C2 Constellation and Navy FORCEnet both promote the use of emerging technology to enhance our ability to obtain a more integrated network capability.

In exploring a more integrated and less stove-piped communications medium between SOAs, the question remains "Can Mesh, MANET, and 802.16 technologies connect the USMC DO, USAF, Navy, and Army through the Global Information Grid (GIG) and enhance the Joint capabilities of our services?" I believe that the combination of Mesh, MANET, and IEEE 802.16 technology is one possible solution. Currently, there is a lack of real-time communications from ground to air when mission is in progress—unless the units are in LOS (Tovar, 2005). Hence, there is sometimes time-delayed coordination in Marine Corps, Air Force, Navy and Army working to destroy targets. The usage of Mesh, MANET, and 802.16 technologies could allow cross-domain distribution of information to USAF, USMC, Navy, and Army platforms so that all units become part of the Network Centric operations. More detail about these technologies will be provided in Chapter IV, V, VI, and VII. However, a quick review of these technologies is pertinent. IEEE 802.16 provides a pool of bandwidth, shared automatically among the users—allowing the network to deliver significant bandwidth-on-demand to many users with a high level of spectrum efficiency (IEEE STD 802.16.2-2001). In addition, IEEE 802.16 is a vendor-neutral standard for radio wide area networks (WAN), and it provides: Routable networks; Stable media access; Broadband capacity measured in micro-seconds (m/s); and Simple Network Management Protocol (SNMP) management. Mesh is a loosely defined term that encompasses abilities of a subscriber station (SS)

to migrate from one base station (BS) to another BS (called Hand-off) and to "daisy-chain" nodes together, usually involving a node acting as BS in one segment and as a SS in another segment, with an auto-configuration ability. In addition, Mesh is a networking capability in which SS broadcast data in the Medium Access Control (MAC) layer to other nodes within the network (Burbank and Kasch, 2006). And, finally, MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure (Sun, 2006). In addition, MANET protocols are enhanced routing protocols designed to deal with volatile routing topologies.

B. DISTRIBUTED OPERATIONS

Distributed Operations (DO) describes an operating approach that will create an advantage over an adversary through the deliberate use of separation and coordinated, interdependent, tactical actions enabled by increased access to functional support, as well as by enhanced combat capabilities at the small-unit level. The essence of this concept lies in the capacity for coordinated action by dispersed units, throughout the breadth and depth of the battlespace, ordered and connected within an operational design focused on a common aim (Hagee, 2005).

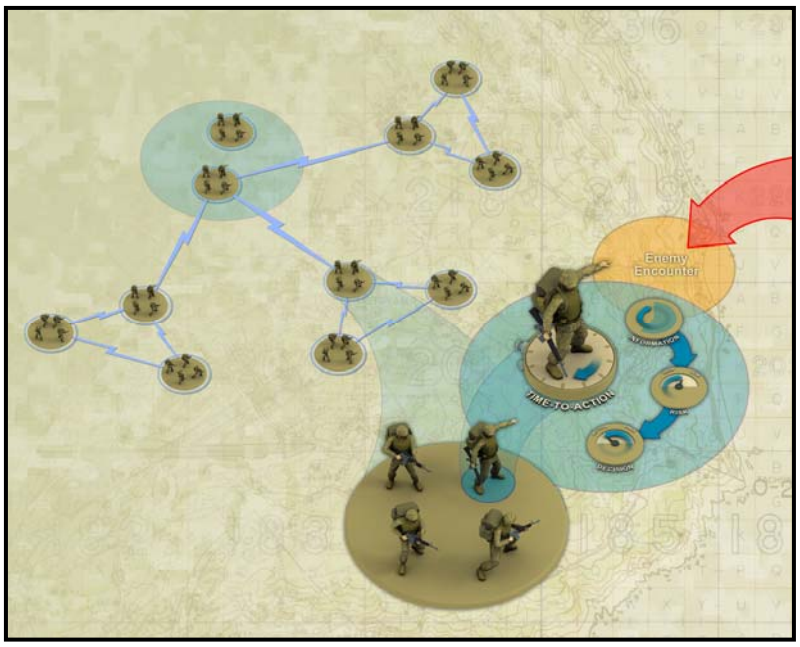

Figure 1. Distributed Operations Communications (From: MCWL, 2006)

In Figure 1, the structure and complexity of a DO unit is normative of a Marine platoon. However, the operational ability of that unit will be increased, due to the C2 capabilities gained with COTS technology. In order to minimize research and development cost and fielding time, the Marine Corps will exploit existing capabilities—"off the shelf" technology—to the greatest extent possible (MCDP 1, 1997). The employment of COTS Mesh and MANET equipment in DO is an avenue that could provide the ability to have deliberate separation of squads while maintaining the cohesive, coordinated tactical actions. Both Mesh and MANET technology offer a network that could support a dynamic, rapidly-changing, and random wireless end system connecting to a wired network infrastructure. These information end systems make up the sense, decide, and act (SDA) end nodes and the networks that connect them together (Buddenberg, 2005). In the DO concept, the forward deployed unit acts as the SDA node. The DO concept implementation is basing its implementation on building modularization into the systems access to the GIG infrastructure. Modularization is building of end systems so that each can connect and operate in a transparent means to the network infrastructure based on IEEE standards. The end systems can assimilate to the GIG by connection points that are compatible to entry point

routers. This seamless entry into the network infrastructure through the routers would make these end systems good network citizens. Good network citizenship encompasses (Buddenberg, 2005):

- Local Area Network (LAN) interface
- An enveloping definition (MIME or XML)
- A means of authentication and encrypting data (S/MIME, XML-sign and –crypt)
- Setting Differentiated Services Code Points (DSCP) on existing datagrams for QoS purposes
- An Simple Network Management Protocol (SNMP) agent that affords both local and remote manageability

A LAN interface is the entry point into the network, and the enveloping definition that allows information to enter the network is the Differentiated Services Code Points (DSCP). DSCP is a new model in which traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. The DSCP field is defined as an unstructured field to facilitate the definition of future per-hop behaviors (RFC 2474). DSCP is the six most significant bits of the DiffServ field. The standardized DiffServ field of the packet is marked with a value so that the packet receives a particular forwarding treatment or Per-Hop-Behavior (PHB), at each network node. The PHB Group is called Assured Forwarding (AF). The AF PHB group provides delivery of IP packets in four independently forwarded AF classes (RFC 2597). The importance of the attaching DSCP for Quality of Service (QoS) is that AF PHB assures forwarding of IP packets over the Internet. In a typical application, a company uses the Internet to interconnect its geographically distributed sites and wants an assurance that IP packets within this intranet are forwarded with high probability (RFC 2597) of success. In this fashion of QoS, the military could use the ad hoc products that act as good network citizens to close the gap and bridge their architectures so that the GIG could act as the thread amongst the different SOAs. Then, the routers at the edge of the network could classify packets and

mark them with the DSCP value in a DiffServ network and let the PHB behavior for the packets provide the appropriate QoS treatment (Cisco Systems, 2006). The following picture gives an example of routers attaching to the GIG, with the independent nodes or ad hoc network connections to the routers.

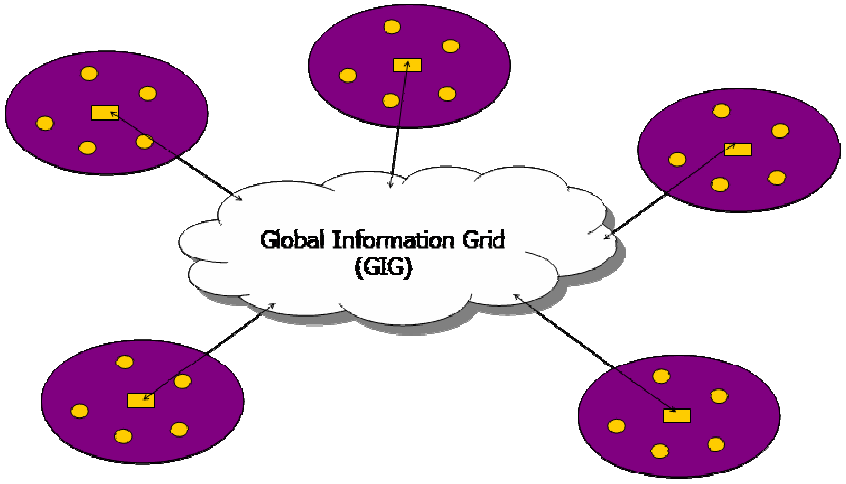

Figure 2. MANET connecting to GIG (From: JHU/APL, 2006)

According to RFC 2475, the SOAs (defined in Chapter III) using DSCP:

- should work with existing applications without the need for application programming interface changes or host software modifications (assuming suitable deployment of classifiers, markers, and other traffic conditioning functions)
- should decouple traffic conditioning and service provisioning functions from forwarding behaviors implemented within the core network nodes
- should not depend on hop-by-hop application signaling
- should require only a small set of forwarding behaviors whose implementation complexity does not dominate the cost of a network device, and which will not introduce bottlenecks for future high-speed system implementations
- should avoid per-microflow or per-customer state within core network nodes
- should utilize only aggregated classification state within the network core

- should permit simple packet classification implementations in core network nodes (BA classifier)
- should permit reasonable interoperability with non-DS-compliant network nodes
- should accommodate incremental deployment.

All of these aspects are conducive to MANET technologies acting as a good network citizen for edge units. In addition, SNMP is an Internet-standard protocol for managing devices on IP networks. The devices that support SNMP include routers, switches, servers, workstations, printers, and modem racks. SNMP can be used to control these devices and even send pages or take automatic action if problems arise (Mauro and Schmidt, 2001). The networking and implementation of these end systems as good network citizens will allow for central management and a COP that details what units are connected or not. Although this is a brief overview of their capabilities for DO, Mesh and MANET will be further defined in later chapters.

C. JOINT FIRES

Joint and coalition actions involve many diverse architectures and independent weapon systems that, ideally, cooperate and communicate to carry out missions. Current C2 systems, however, typically cannot communicate within a single plane for Joint Fires. Joint Fires occurs when two or more services use lethal and non-lethal weapons in coordinated action toward a common objective (US JFCOM, 2005). Under NCW, Joint Fires need to communicate, collaborate and share a common picture, composed of voice and data as well as imagery, at all echelons (Tovar, 2005). Joint-service and coalition operations, such as close air support, require shared approaches and technologies (Navy League of the US, 2005). In addition to approaches and technologies, Joint and coalition operations need cross-domain interoperation that enables the ability to respond to unexpected events in a timely and effective manner (SAB-TR-05-03, 2005). Instead of focusing on providing whole systems that communicate and building entirely new infrastructures to support a common

communications plane, the Joint Fires environment should focus on COTS technology overlay that incorporates ability for the military to exploit our common reliance on an IP backbone for information transport. Successful information integration efforts depend critically on elimination of barriers to information sharing across the enterprise (SAB-TR-05-03, 2005). The bigger challenge is tying these integration efforts together in a shared global information network, linking ground, air, and sea forces (Navy League of the US, 2005). Currently, our military infrastructures address multiple means to call for fire in US military infrastructure. The commonality with all these systems is their reliance on point-to-point communications. Figure 3 shows point-to-point and point-to-multipoint communications.

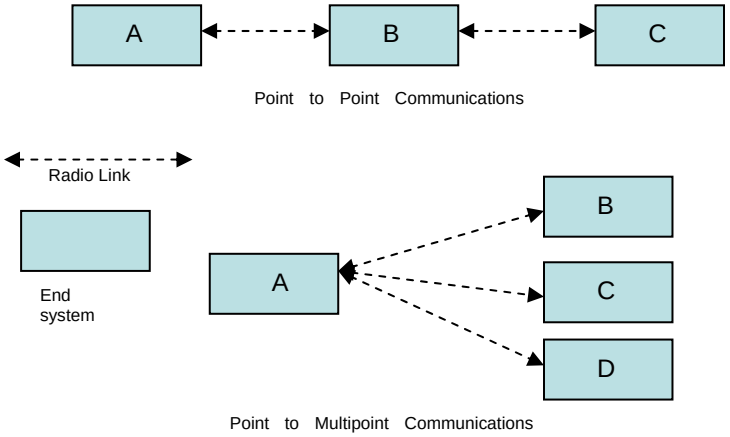

Figure 3. Radio Communication Links

As illustrated in Figure 3 above, if a point-to-point link fails, there is no connecting or alternate path for the information to travel from A to C. So, from a network perspective, there is no actual networking in point-to-point, only a huge number of direct radio links. However, radio links that have an IP-based technical overlay have the ability to link directly into the IP network infrastructure if their connection to a GIG entry point is not severed. The connection between the end system and GIG entry point is a Physcial layer connection. The data links into the IP network infrastructure at Layer 1 and flows through the intermediate system (Layer 1 up through Layer 3). The following chart depicts an Intermediate System within the OSI model.

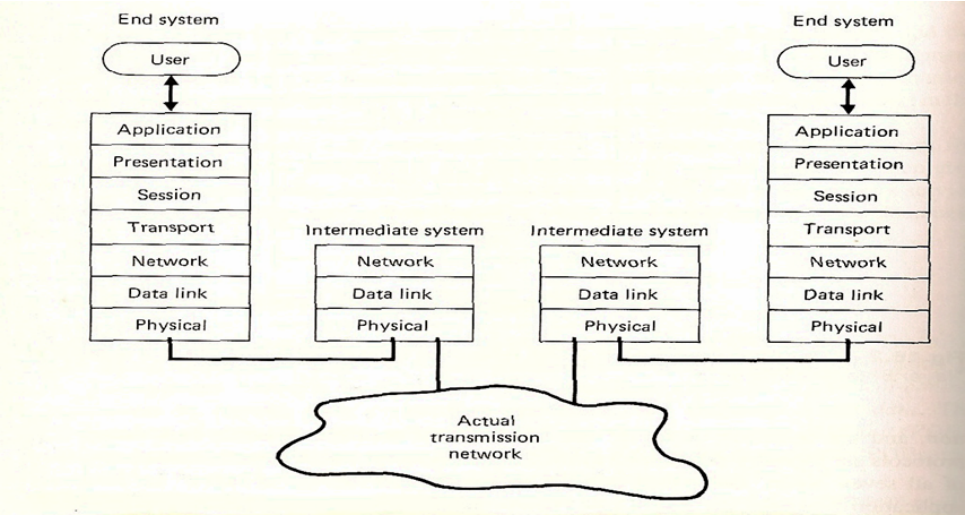

Figure 4. Intermediate System (From: Operating Systems 2nd Ed, H.M. Deitel)

In this Figure 4, the end systems connect through the intermediate system's stack to other systems. The linking of disparate end systems in different SOAs is possible through the Intermediate System. This approach allows the units at the very edge of our networks to communicate with units at the upper levels—that may belong to different SOA. The USAF has stated with its C4ISR Flight Plan and through its lead agencies that the "Airborne Network" is the portion of the C2 Constellation Net that provides communication and enterprise services to, from, or between intermittently connected network subscribers on platforms capable of flight. And, C2 Constellation Net provides capabilities to link airborne platforms with surface and space based network subscriber entry points (AFCA/ESA, 2004). Similarly, the Navy stated that Joint-service and coalition operations, such as close air support, require shared approaches and technologies, and the bigger challenge is tying these and other efforts together in a shared global information network, linking ground, air and sea forces (Navy League of US, 2006). This thesis will demonstrate in Chapter VIII that extensive research and evaluation are required to achieve a smarter means of translating the data from Layer 1 up to Layer 3 of the OSI model (shown in Figure 4).

The current JCAS and Fire Support elements operate on circuit switched (point-to-point and LOS) RF radio network that are being made amenable to IP networking. Yet, if the military implemented Mesh or MANET technology as communications medium at the edge units, there could be seamless interface of information from the Physcial (PHY) layer, through the Medium Access Control (MAC) layer, to the Network Layer, which would allow end-systems to achieve self-forming and self-healing connectivity that IP networking provides. In addition, with the expanding technology enabling Mesh and MANET technologies to communicate with air nodes, there would be a communication tie from ground-to-air, as well as be tied directly to all other components with Mesh and MANET technology. Currently, the only way for the Airborne Network to tie into the current GIG is to connect to some ground node that directly enters the fixed infrastructure of our current GIG architecture. In any JCAS or Joint Fires activity, the marine, soldier, or airman on the ground is our best sensor. Thus, if our military research focused on incorporating Mesh or MANET technologies to obtain land, air, and sea connectivity and addressed the Data Link and Network Layer issues, the edge units could possibly act as building blocks for extending the IP network. These IP building blocks could enhance our ability to deliver JCAS and Joint Fires by centralized command, decentralized execution.

D. SUMMARY

We cannot afford to be unsuccessful in bridging the gaps that we have between ground, air, and sea forces. As noted by Les Aspin and William Dickinson (Snyder, 1993),

> Operation Desert Storm demonstrated that tactical communications are still plagued by incompatibilities and technical limitations….Communications were worse in the field…Multi-service strike packages were difficult or impossible to assemble because various aircraft communicated in different ways over secure voice channels.

The ability to horizontally integrate information from space, air, and ground at a machine-to-machine level will enable the Services (Air Force) to rapidly and

accurately integrate data and information across domains to address time sensitive targets (SAB-TR-05-03, 2005). This addressing of time-sensitive targets and sharing of data across domains would enhance and demonstrate an improvement in our C2. C2 is the nervous system that coordinates the muscles of our national security system, from weaponry to diplomacy (Coakley, 1991). In a tactical engagement, failure in C2 may result in a tactical defeat, because a commander is unable to bring all available forces into action, to apply them efficiently and effectively, or to prevent them from firing on each other (Snyder, 1993). To improve Joint Fires, C2 of our military sources must give commanders better knowledge of what they are up against, what resources are available and how they might be used (Coakley, 1991). A system that can inform a commander—about the status of our own forces, about the location and apparent intentions of an enemy, or about the probable result of alternative courses of action—after only five minutes can be considered a better system than one that requires an hour to produce the same information (Snyder, 1993). Currently, the circuit-switched point-to-point communications between edge units and higher echelons dictates that kind of time in our decision cycle. DO and any other edge unit operations using MANET technologies could have a huge contributing factor to lessoning the communications from hours to minutes. See Figure 5. It illustrates an example of the possible connectivity.

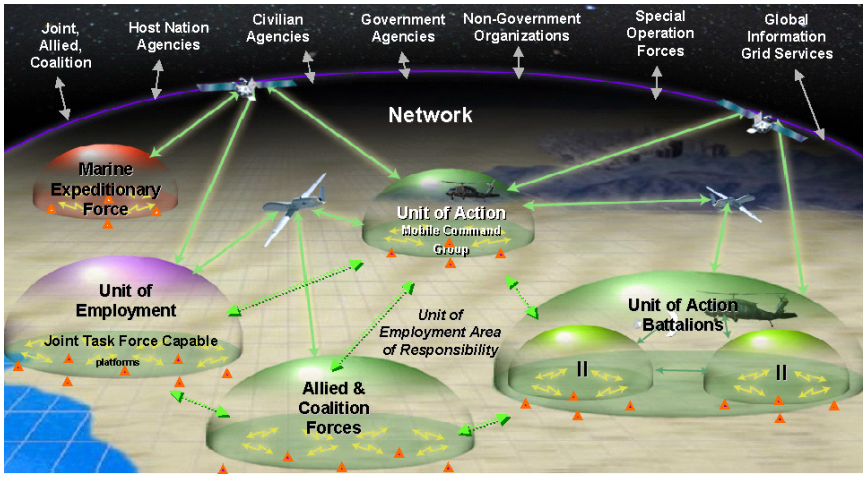

Figure 5. LandWarNet (From: C4ISR Flight Plan, 2004)

In the Figure 5 illustration, DO units, Special Operations Forces (SOF), UAVs, or any edge unit would not control the information; instead, these edge nodes would act as forward air and ground sensors and distribute information to all tiers of C2 infrastructure through GIG connectivity.

III. DOMAIN INTEGRATION

A. INTRODUCTION

Domain Integration is defined as the implementation of (widely) shared functional interfaces between domains that allow (but do not necessarily require) access to use or control resources and capabilities with the domains (SAB-TR-05-03). And, as defined previously, SOA is overall a grouping of services. These services involve communicating through the exchange of data elements or the services could include two or more services correlating to orchestrate an event or plan (Service-architecture.com, 2007). By improving Domain Integration and SOAs integration, the military will be enhancing our ability to achieve a networked Joint Technical Architecture (JTA). JTA is defined as a common set of standards and guidelines to be used in all C4I systems and interfaces of C4I (JP 1-02). The following illustration provides a high-level JTA.

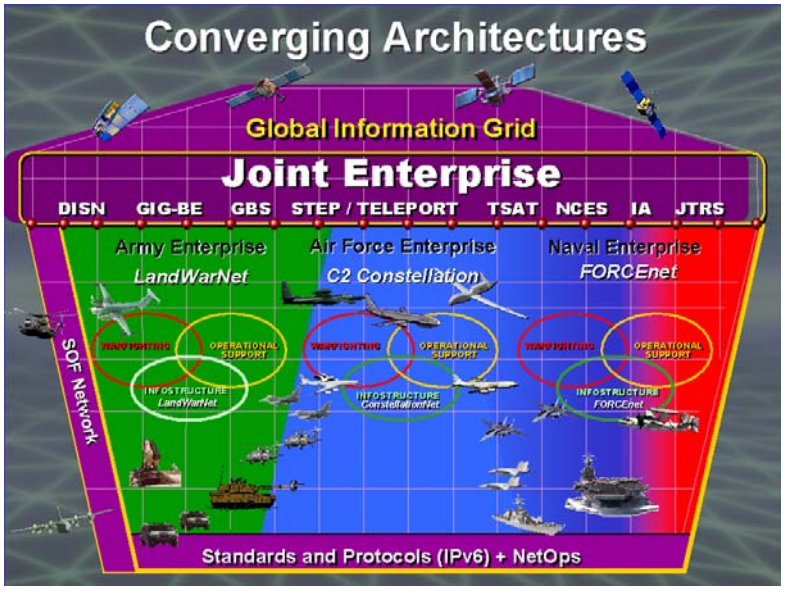

Figure 6. Joint Technical Architecture (From: C4ISR Flight Plan, 2004)

Joint military forces need a networked JTA capability to decentralize our decision-making, so small units can locate, close with, and destroy asymmetric threats (Tovar, 2005). These small units would consist of Marine DO units, SOF, or Combat Aircraft at the edge of our network infrastructure or BLOS. A focal

point of any small edge unit would be to disseminate information to all echelons of the C2 chain. However, the dissemination of the information is not to give additional controlling power to the sergeant, shooter; or artillery man; it is to provide better situational awareness from the best sensor—our edge components—to the decision makers, the commanders--who understand the strategic implications of redirecting military firepower. With this enhanced situational awareness, the commanders can coordinate with the same set of data at all echelons. This decentralized knowledge base would allow the land commander and air commander to make decisions based on Common Operational Picture (COP) that is minutes old instead of hours. The C2 offered by the increased information dissemination would allow Joint Fires to be more effectively employed and better directed. Future warfare, characterized by faster operations tempo, requires a new orientation based not on centralized control but on greater decentralized control and more flexible organizational orientation (Roman, 1997).

B. DOMAIN INTEGRATION

To achieve the commander's intent, services must have domain integration. Here, Mesh and MANET technology would improve domain integration and not decapitate the strategic coordination process. Due to the nature of Optimized Link State Routing (OLSR) in mesh networking, mesh networking is perfect for the "Last Mile" operations in the military environment where joint combined maneuvers are required when you combine ground and air as part of Airborne Networking (AN). Clausen and Jaquet relay interesting facts about OLSR.

> OLSR is a proactive routing protocol for mobile ad hoc networks. The denser a network, the more optimization can be achieved. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route packets. OLSR means that communications would be fluid because no additional control traffic is generated in this situation since routes are maintained for all known destinations at all times (Clausen and Jaquet, 2003).

The use of this technology would improve the ability for the different SOAs to handle the diverse systems and improve the maneuverability at the edge of our networks. To make these improvements, there are three aspects of domain integration that requires addressing: 1. Infrastructure integration, 2. Information integration, 3. Process integration (SAB-TR-05-03, 2005).

1. Infrastructure Integration

Infrastructure integration is the building of end systems where data exchanges across system boundaries. To network the diverse end systems and supervise the maneuverability of the edge units, infrastructure integration must occur in all services. The SOAs could integrate by bridging their service architectures through COTS technologies. By using the emerging COTS technologies, the military could leverage the many benefits of commercial standards-based technology, such as economies of scale and open-standard technology (Burbank and Kasch, 2006). These open standard technologies would access the GIG through 802.16 and Mobile Ad Hoc products that will use the standard OSI model infrastructure and enable their end systems to connect directly to the static backbone infrastructure or other service end nodes.

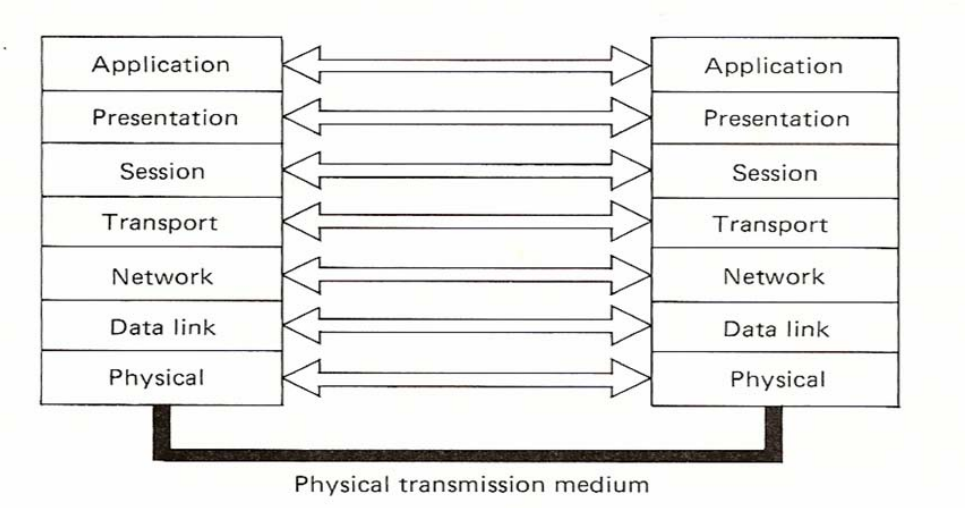

Figure 7. OSI Model (From: Operating Systems 2nd Ed, H.M. Deitel)

To access the static entry points for the GIG, the intermediate system uses a transport service bridge, service emulation, and/or network service

tunneling at the Data Link and Network layer. These network service approaches highlight an interesting class of coexistence techniques based on service emulation rather than protocol translation (Rose, 1988). In the diagram above, the Physical layer provides the logical connection between the Data link layer of two or more systems. The Physical layer makes use of transmission media whose characteristics are not part of the OSI model (McClelland, 1982). With the underlying physical connections using common IEEE standards, the crux of infrastructure integration occurs at the interconnection of Network to Transport layers. The Network layer is the location in the OSI stack where address assignments are made and packets are forwarded from one end of the network to the other. The Transport layer is where reliable transmission and rudimentary transit decisions are made using complex protocols. By interconnecting these layers through emerging technology, the military achieves GIG-wide tunneling and service emulation to maintain information in standard OSI structure, so the communications take on normative characteristics of an IP infrastructure.

2. Information Integration

Information integration is the building of network architecture where data freely moves between all echelons of the military structure and data exchange helps build a single coherent COP. With information integration in a domain, the very nature of controlling information defeats the optimum use of the information…Controlled information becomes slow information. Information must move with a degree of freedom at all levels of command to better balance decision making at all levels of command (Roman, 1997). With emerging mobile ad hoc technologies, the military could enhance the ability for the information to flow from the tip of the spear back to the home base of operations. C2 of information at the tip of the spear relies on information systems to provide a COP to separated commanders, a COP that itself rely on doctrine, teamwork, and information exchange (Snyder, 1993). Commanders whose forces are in contact with those of an enemy should indeed be receiving information about the enemy from those forces (Snyder, 1993). As mentioned previously, all information

integration systems are made up of Sense Decide and Act (SDA) nodes. These SDA nodes could be soldiers, marines, and airman; or UAVs, Predators, Rotary, and Fixed Winged assets. No matter the mission, the objective is to place the mission sensors, the mission decision support systems, and the mission actors (weapons) in an inherently interoperable position (Buddenberg, 2005). At the tactical level, the improvement of C2 information integration by SDA nodes use of COTS technology could improve the call for fire, the techniques for fire, the operations of weapons and equipment, and the tactical movement techniques. For implementation of Mesh, MANET, and 802.16 capabilities, the military must believe that success can be measured according to previous metrics taken for static infrastructures. The criteria are Performance, Flexibility, Transparency, and Amenability (Rose, 1988).

Performance: How well does the strategy perform in terms of both throughput and latency? How does the strategy impact the performance of other applications running in the network?

Flexibility: What is the range of applicability of the strategy? Is a special-purpose system required for each application, or can one general-purpose system serve the needs of a wide range of applications?

Transparency: Is it possible for end-users to be unaware that the coexistence/transition strategy is “in the loop”?

Amenability: How manageable is the strategy? Does the strategy impose additional administrative burden on the network operator.

Since our communications decision authorities can answer these questions by applying Mesh, MANET, and IEEE 802.16 technologies, the military should consider using these emerging technologies to provide information integration. The following figure illustrates a high-level snapshot of a possible information infrastructure for the military JTA information integration.

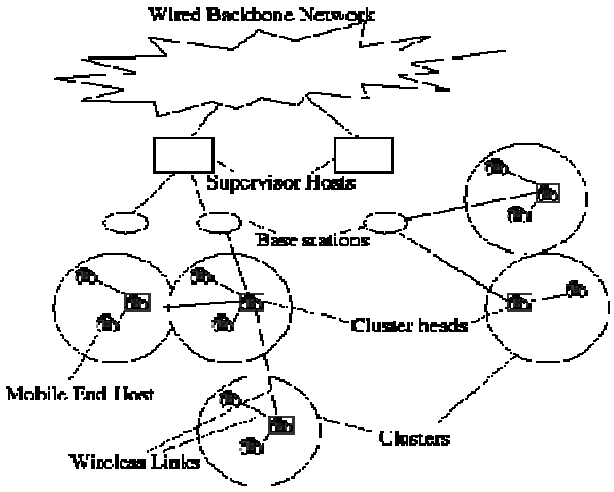

Figure 8. JTA: Wired to Mobile Network (NPS CWNA Course, 2006)

3. Process Integration

Process integration allows end systems to exchange mission-data between service components for collaboration. The military needs radio-WANs to connect these disparate end systems in different SOAs. These radio links would need to pull together wired backbones and extend the internet to reach our mobile platforms, as illustrated in Figure 8. By pulling together these backbones, process integration would enhance interoperability. Interoperability is the foundation of effective joint, multinational, and interagency operations. The joint force has made significant progress toward achieving an optimum level of interoperability, but there must be a concerted effort toward continued improvement (JP 1-02).

C. GLOBAL INFORMATION GRID (GIG)

The GIG is critical to domain integration. The GIG is defined as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), system data,

security services, and other associated services necessary to achieve information superiority for the United States military (Wikipedia). A prerequisite for a widespread and successful deployment of proactive ad-hoc networking technology is its ability to achieve easy access to the Internet (Englestad, Tonnesen, Hafslund, and Egeland; 2005). With the implementation of GIG-BE, the Department of Defene (DoD) should have multiple entry points throughout the world to provide access to edge units. GIG-BE provides a secure, robust, optical terrestrial network that delivers very high-speed classified and unclassified IP services to key operating locations worldwide. The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) vision is a "color to every base," physically diverse network access, optical mesh upgrades for the backbone network, and regional upgrades, where needed. "A color to every base" implies that every site has an OC-192 (10 gigabits per second) of useable IP dedicated to that site (Wikipedia). By enhancing the deployment of fiber infrastructure and providing entry points through Defense Information Services Agency (DISA) sites and satellites, the DoD has created the ability for edge organizations to possibly exchange data with command centers real-time.

D. CONCLUSION

Thomas P. Coakley states "Whoever can make and implement his decisions consistently faster gains tremendous, often decisive advantage" (Coakley, 1991). This statement recognizes that improvement in the SOAs communications grid enables an improvement in the C2 process. Hence, the aforementioned addition of COTS to improve the C2 process for dissemination of information is critical for America to continue to advance in its ability to wage war. War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously. Like war itself, our approach to warfighting must evolve. If we cease to refine, expand, and improve our profession, we risk becoming outdated, stagnant, and defeated (MCDP 1, 1997). By using COTS products to achieve domain interoperation at

edge units, the military would be well on it way to achieving domain integration and fulfilling our combined Joint Vision 2020 goal. In addition, the military would be signaling that we are cognizant that, as the hardware of war improves through technological development, so must the tactical, operational, and strategic usage adapt to its improved capabilities (MCDP 1, 1997). Now that Chapters I, II, and III have provided a conceptual overview, Chapters IV will start the technical overview by detailing the layer modularity of the IEEE 802.16 technology.

IV. LAYER MODULARITY

A. INTRODUCTION

In the movement of information through nodes in a networked environment, the layer modularity of the MAC and PHY layer are critical elements in the transmittal of data. The critical points are the interconnection points between the layers. The Service Access Point (SAP) is the point in a protocol where the services of a lower layer are available to its next higher layer (IEEE Std 802.16-2004), and it acts as the connection between these layers and contributes to the efficiency (Figure 9).

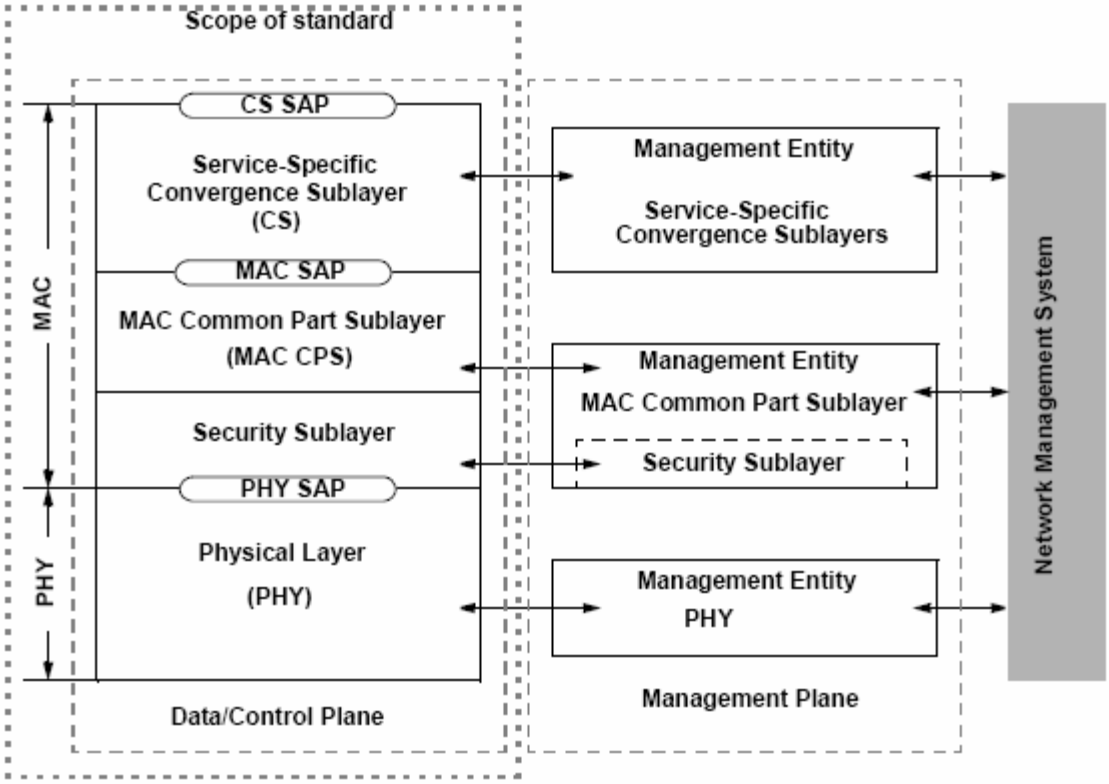

Figure 9. IEEE Std 802.16 protocol layering, showing SAPs (From: IEEE Std 802.16-2004)

In the MAC layer, the Service Access Point (SAP) key role is that it is the interface definition between PHY layer to MAC Layer, and the MAC Layer to the Data Link layer. The importance of SAP in layer modularity is that it does not

allow the actions of the each individual layer to affect the other layer. However, it does allow modifications within a particular layer. The SAP is critical to communication because in the MAC, the SAP classifies external network Service Data Units (SDUs) and associating them to the proper MAC services flow identifier (SFID) and connection identifier (CID). Once the MAC sets SDUs to SFID and CID, the end-system starts to communicate with the modification up the protocol stack. The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It receives data from the various CSs, through the MAC SAP, classified to particular MAC connections, which, in turn, provides Quality of Service (QoS) to the transmission and scheduling of data over the PHY layer (IEEE Std 802.16-2004).

B. IMPORTANCE OF LAYER MODULARITY

There are some key reasons why the layer modularity approach of IEEE 802.16 is appropriate for the flexible environment of Joint networking. The IEEE 802.16 MAC layer modularity model depicted is based on the IEEE 802.3 standard, which has provided solid communications services over the past decade. Thus, the usage of this technology does not require any far-fetched actions to make it amenable to absorbing technology advances. Ideally, IEEE 802.16 will hopefully provide the same longevity and solid communication. In addition, because IEEE 802.16 is built on top of the characteristics of 802.3, networked systems could be upgraded in the PHY layer without changing or adding any protocols above the MAC layer. The ability to enhance in this manner offers good possibilities:

- DoD can build military-specific PHY implementations that respect the MAC/PHY SAP without any changes cascading through the rest of the protocol stack.

- DoD can manipulate communications attributes in PHY without altering the rest of the standard as a means of rapidly incorporating new technology—i.e., Futureproofing.
- Since the layering structure in IEEE 802.16 is drawn from that in IEEE 802.3, DoD technologist can some longevity.

C. CS SAP

The Convergence Sublayer (CS) SAP is the interface definition between the MAC layer and Network layer. The key role of the CS SAP is that it insulates the development of PHY and MAC layer protocols that reside in the Subscriber Stations (SS) or Sense, Decide, and Act (SDA) nodes from layer 3-7 protocols.

From a CS SAP, centralized scheduling configuration is sent to the MAC entity in the BS (IEEE Std 802.16-2004). This centralized scheduling configuration prioritizes the resources for communications. In centralized scheduling, maintenance windows are granted in a more centralized manner. Therefore, the BS gathers resource requests from all SSs within range. Then, the scheduler allocates the timeslots in the maintenance window so the SSs can communicate in an efficient manner (IEEE Std 802.16-2004).

D. MAC SAP

The MAC SAP is the interface definition between the Service-Specific Convergence Sublayer (CS) and the MAC Common Part Sublayer (CPS). The importance of the MAC SAP is that it allows services between the CS and MAC CPS. These services enable MAC CPS to provide the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance.

The MAC SAP is also responsible for delivering the MAC SDU generated in its CS to another SS MAC SAP from the point where the CS connects to MAP SAP. Moreover, the MAC SAP is responsible for delivery of the MAC SDU to

peer MAC SAP in accordance with the QoS, fragmentation, concatenation, and other transport functions associated with a particular connection characteristic. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity (IEEE Std 802.16-2004). By doing the connections in this manner, link connection is defined when the connection is created by the MAC SAP and the connection to the other SS MAC SAP is established without interference and has received a dedicated time slot for seamless communications. The importance of the action is that the MAC SAP acts as the protection point from the PHY layer manipulations of the radio frequencies modifications and PHY definition changes. (IEEE Std 802.16-2004) and maintains dedicated connections for improved QoS, stability, and better bandwidth efficiency.

E. PHY SAP

The PHY SAP is the interface definition between PHY layer and the MAC layer. From the PHY layer to the MAC layer, the PHY SAP allows data, PHY control, and statistics to transfer between the MAC CPS and the PHY. This data exchange is implementation specific and allows change to the physical media interface definition. (IEEE Std 802.16-2004). The key is that any radio frequency-specific requirements, such as military-specific spectrum, analog bandwidth requirements, Low Probability of Detection (LPD)/Low Probability of Intercept (LPI) features, link-layer encryption, etc… implements wholly within PHY layer, which provides flexibility. Once this change is administered and the end-system starts to communicate with the modification up the protocol stack, the Protocol Data Units (PDU) and Service Data Units (SDU) within the MAC layer operate in a device independent fashion, and the SDA node does not have to be changed. The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It receives data from the various CSs, through the MAC SAP, classified to particular MAC connections, which, in turn, provides Quality of Service (QoS) to the transmission and scheduling of data over the PHY layer

(IEEE Std 802.16-2004). The point is that these sublayers – the entire MAC protocol – need not be changed either to adapt to specific military situations or to introduce new PHY technology.

F. CONCLUSION

We have provided a cogent articulation of the MAC layer modularity structure that operates in a SDA node. This focus on layer modularity provides details on the PHY SAP, MAC SAP, and CS SAP and presents insight on their importance to the transfer of data within the end system and network. The MAC/PHY SAP insulates the physical media dependent radio frequency issues from the framing (Physical Media Interface) problems and access issues associated with the MAC layer. And, CS SAP is the interface definition between the MAC layer and Network layer which allows the CS SAP to insulate the development of PHY and MAC layer protocols that reside in the SDA nodes from routing protocols affiliated with the Layer 3 and the application protocols affiliated with Layer 4-7. In addition to the efficient communications enabled by these SAPs, the layer modularity of the MAC/PHY layers also endows the military with the ability to manipulate the capabilities of end systems by changing specifications in the PHY layer without things cascading through the system. Hence, layer modularity futureproofs the SDA nodes because it allows adaptation of what started out as a commercial standard to military purposes, in large part, by only modifying the PHY layer of the node.

In conclusion, this chapter focuses on the layer modularity of MAC and PHY layer in a radio network standard, IEEE Std 802.16-2004. And, it fixes in place the layer modularity concept. With this concept in hand, the following chapter walks through a comparison between the well-modularized IEEE 802.16 standard and the design of the Mil-Std-188-220 military standard on a peer basis -- e.g., MAC to MAC. The MAC layer comparison permits grasping of the differences in providing an overlay to legacy technology (Mil-Std-188-220)

compared to using a COTS technology (IEEE 802.16) formulated to communicate with bandwidth efficiency, stability, and QoS in the GIG environment.

V. MAC TO MAC COMPARISON

A. INTRODUCTION

In the Mil-Std-188-220 Combat Net Radio (CNR) environment, the MAC in Mil-Std-188-220 uses Carrier Sense Multiple Access (CSMA) network access (Mil-Std-188-220, 2001). CSMA is a MAC protocol that requires the system check the communications medium to assess if it currently being used before trying to transmit. This protocol attempts to prevent the collision of packets that could cause the system to drop data. In using CSMA, a node can communicate with another subscriber station (SS) without having to listen to all the SSs at the same time. However, all of the SSs communicate with the base station (BS). Therefore, if there are multiple systems in the area, SSs could attempt to send information to another node simultaneously. This increased traffic load translates into increased collisions. Eventually, the collisions beget more collisions and the increased congestion causes the network to grind to a halt. This collision problem causes instability issues:

- The network segment becomes bandwidth inefficient and stalls.
- The network uses small amounts of baseband capacity because SSs are spending their transmit time fighting for access.
- QoS control weakens due to the inability to distinguish the needs of one SS from another.

Hence, the CNR environment would degrade quickly. The inefficiency comes when two SS are unable to communicate with each other, so their polling of network gives a false impression that the medium is free, when it is actually being used. In short, the CSMA portion of the CSMA/Collision Detection (CD) protocol fails the network.

However, IEEE 802.16 does not operate in the same fashion as the Mil-Std-188-220 technology. To prevent bandwidth inefficiency in an IEEE 802.16 communication network, each SS is assigned a particular physical slot (PS). A

PS is a unit of time, dependent on the PHY specification, for allocating bandwidth (IEEE Std 802.16-2004), so there will be no collisions.

Within this allocation of bandwidth, a SS requests uplink bandwidth on a per connection basis (implicitly identifying the service flow). Bandwidth is granted by the BS to a SS as an aggregate of grants in response to per connection requests from the SS (IEEE Std 802.16-2004). The IEEE Std 802.16-2004 defines service flow as a unidirectional flow of MAC SDUs on a connection that is provided a particular QoS. These different unidirectional flows are possible because the communication between BS and SS is managed by Time Division Multiplexing Access (TDMA) in an uplink and a downlink fashion. TDMA is defined as a burst of data using PHY parameters, determined by the Downlink Interval Usage Code (DIUC) or Uplink Interval Usage Code (UIUC) (IEEE Std 802.16-2004). In the communications between the BS and SS there is a constant monitoring process of the uplink and downlink burst by the BS. The BS controls and administers the profiles that allow the SS access the channel for communication. This constant monitoring disengages the need for acknowledgement, since the SS will always be guaranteed a timeslot by contention opportunities (Eklund, Marks, Stanwood, and Wang, 2002). These actions by the IEEE 802.16 technology allow the network to:

- Maintain stability.
- Achieve a high-rate of bandwidth efficiency.
- Do a real-time polling service to maintain QoS for Data and Voice transmission.

To give a better insight into the differences between Mil-Std-188-220 and IEEE 802.16, we next focus on: Stability; Bandwidth Efficiency; and QoS.

B. MAC-TO-MAC: STABILITY, BANDWIDTH EFFICIENCY, AND QOS COMPARISON

1. Stability

In Mil-Std-188-220, CSMA allows over subscription by the SSs. As the number of SSs increase in the CNR, the dropping of packets during the transmittal of information grows and the number of collisions grows as well. The increased congestion of colliding packets increases the likelihood of more collisions due to a rate greater than linear. Thus, the process of transmission, collision, and retransmission creates and unstable network segment that eventually grinds to a halt. However, in an 802.16 network, stability is maintained because each SS is allocated its own slot of bandwidth. The MAC uses contention opportunities to do bandwidth-slot allocation, which does not allow collisions and allows the SS to enter the network. Because collisions are eliminated by design, the communications system maintains its stability throughout operation.

2. Bandwidth Efficiency

Mil-Std-188-220 usage of CSMA reduces its ability maintain a high rate of bandwidth efficiency due to the instability in the network. In the CNR environment, the network area of coverage could be larger than a single access point. Therefore, the baseband efficiency would eventually decrease as the number of collisions and retransmissions grow. CSMA is a contention based protocol that keeps each SS continually battling for access and sending information. However, in IEEE 802.16, bandwidth efficiency is maintained at a high level due to each SS accessing the network through contention opportunities. After the SS enters the network, it is moved out of the contention window into its own exclusive timeslot. This timeslot is assigned by the BS and prevents the SS from contending for access. This means that the SS can transmit data disassociated from having to acquire access to the media. This process means that every SS sends its data along a dedicated bandwidth slot that allows the transmission pipe to operate at a high level of efficiency.

3. QoS

Mil-Std-188-220 uses contention management in CSMA for QoS. Contention management allows each SS to struggle for access to the network. The contesting SSs attempt to transmit to transmit data when it believes the network is clear. However, any SS that is polling the network at the same time will contend for the space as well, which will cause a collision. Thus, the process of transmission, collision, and retransmission will continue until the network grinds to a halt. Herein, lies the problem with the contention access method. However, in the IEEE 802.16 environment, the SS, with its exclusive timeslots, is guaranteed access once on the network. The BS provides the SS a particular physical time slot. The timeslot of SS enables it to transfer data efficiently and in a non-contention basis. Therefore, the network does not experience the collisions and retransmission issues associated with CSMA.

C. CONCLUSION

This chapter has highlighted some of the differences between Mil-Std-188-220 and IEEE 802.16. These differences are in these technologies ability to stabilize a network, maintain bandwidth efficiency, and maintain QoS control. The review of the Mil-Std-188-220 reveals that the standard cannot maintain a high level of efficiency because of CSMA. CSMA is easy to implement, but it requires that each SS communicate with the BS. This requirement of communication with the BS is necessary for effectiveness, but it causes inefficiency in the system. The inefficiency is generated when two or more SS transmit data into a network simultaneously. These simultaneous attempts at communication increase collision and retransmission problem. These unstable and flawed network behaviors increase stalling, promote bandwidth inefficiency, and cause an inability to maintain QoS. Review of IEEE 802.16 reveals that the technology's usage of contention opportunities gives SSs exclusive timeslot. These exclusive timeslots are assigned by the BS and prevents the SS from contending for access. This means that the SS can transmit information and not contend for access. Transmittal of information in this fashion is well-suited to

handle a dynamic environment and provide a robust communication medium that is stable, bandwidth efficient, and allows for good QoS.

Now that the technical details of IEEE 802.16 Layer Modularity and a MAC-to-MAC Comparison of IEEE 802.16 to Mil-Std-188-220 are complete, the following two chapters will discuss MANET and Mesh. In addition, the chapters will highlight operations that could enhance Joint communications in a distributed environment.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. MOBILE AD HOC NETWORK (MANET)

A. INTRODUCTION

Ulysses S. Grant stated:

> The art of war is simple enough. Find out where the enemy is. Get at him as soon as you can. Strike at him as hard as you can and as often as you can, and keep moving on.

As a part of C2 process to carry out Grant's art of war, a MANET should be able to assist the military in striking the enemy quickly with Joint arms. The Joint arms concept relies on the shared understanding of separated commanders, an understanding that itself relies on doctrine, teamwork, and information exchange. In a tactical engagement, failure in C2 may result in a tactical defeat, because a commander is unable to bring all available forces into action, to apply them efficiently and effectively, or to prevent them from firing on each other (Snyder, 1993); hence, the reason for using MANET and comparable technologies for Joint networking C2 among DO, JCAS, and Joint Fires.

B. DEFINITION

A MANET is a self-configuring network of mobile routers and associated hosts connected by wireless links—the union of which form an arbitrary topology. The associated hosts and ends nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger network. By using MANET, our Joint forces would be gaining an inherently joint communications medium that would enable each edge node to communicate with each other while still having the capability to connect back to the service access points and command centers.

A characteristic of MANET is that it has different states of operation. The states of operation can be addressed in a taxonomy based on the rate of connections/disconnections. See Figure 10.

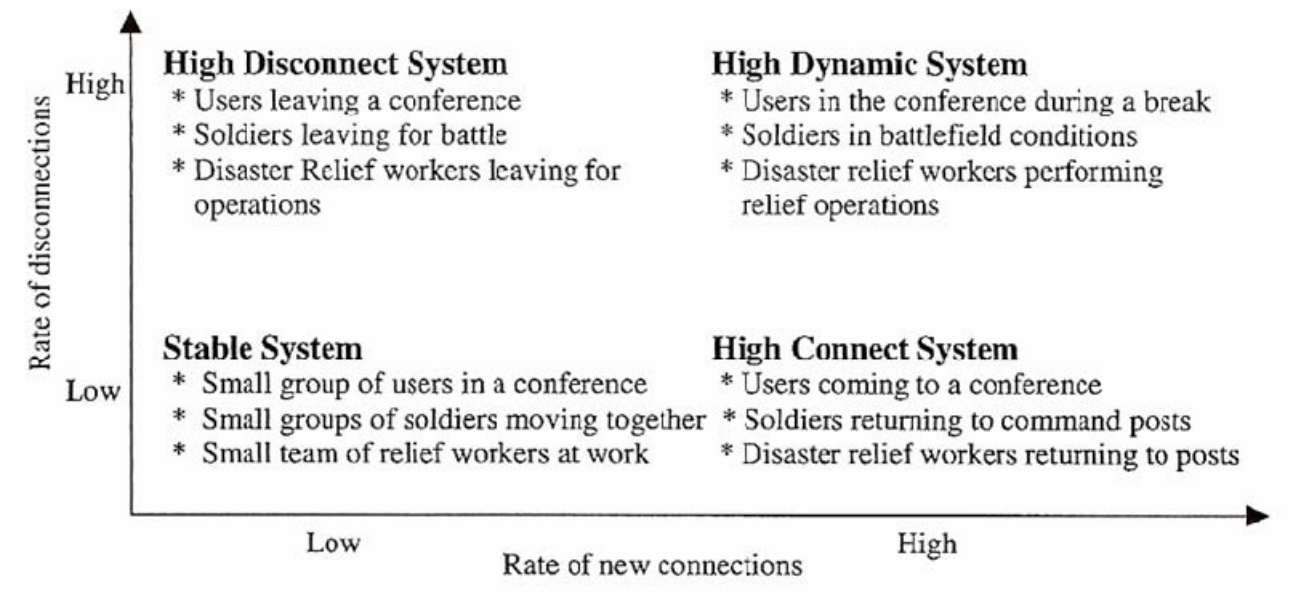

Figure 10. Taxonomy of stages in ad hoc networking (From: Radhakrishnan, Racherla, Sekharan, Roa, and Batsell; 2003)

In a MANET, a state or phase can be:

- *Stable* with low rate of disconnections and connections
- *High connection* with a high rate of connections and low rate of disconnection
- *High disconnections* with a high rate of disconnections low rate of connections; or
- *Highly dynamic* with high rate of disconnections as well as connections.
- And, a single network may operate in different states at different times, or different regions of the network may operate in different modes at the same time (Radhakrishnan, Racherla, Sekharan, Roa, and Batsell; 2003).

Within the bounds of these states or phases, ad hoc networks have advantages in that they:

- Can require less transmit power (for longer battery life).
- Are easy and fast to deploy.
- Have performance that is not critically dependent on infrastructure.
- Can have higher frequency reuse for higher capacity (Winters, 2006).

Once these ad hoc networks, with their different states and advantages, are bound and broadband technologies are connected at Layer 3, the networks promote ubiquitous communications. This ubiquitous communication ties the C2 structure in the command centers to the forces operating on the edge of the network. This virtual binding will enhance the lethality of ground units and air units. The critical feature that enhances the lethality is the robust battlefield awareness through dissemination of information to all levels of the hierarchy. There are a variety of useful scenarios. One such example is a forward deployed DO or SOF unit establishing links with an air node for JCAS and with a TOC to relay coordinates to an artillery unit for Joint Fires. This example will be detailed in the Chapter VIII: Experiment and Equipment Overview.

C. ANALYSIS

In MANETs, a protocol defined as Internet Group Management Protocol (IGMP) uses a routing algorithm so that each node can inform all other systems about which Network layer addresses are being listened to by the node's neighbors. In addition, it is used at Layer 3 to forward IP multicast traffic to all concerned routers. IGMP creates the ability for end nodes to inform their adjacent nodes about the Network layer addresses they wish to receive. When the data packet is transmitted with the network layer address as its destination, the packet propagates through the network based on the source address of the packet (Perlman, 1992). By using protocols like IGMP for its mode operation, MANETs poll networks for routers to deliver information throughout the network. Yet, even with IGMP, the delivery of data could have issues when a large hop count occurs because a number of loops were created due to datagrams going

through the same router greater than once. The time to live (TTL) field in datagram headers manages this problem. TTL field controls how long a router will cache information. It tells routers to throw away datagrams whose TTL values have timed out. One way MANET combats the issue of timing out is by using the Open Link State Routing (OLSR) protocol. The OLSR protocol has a plugin capability that interacts with end system applications and uses multipoint relays (MPR) flooding (see Figure 11).

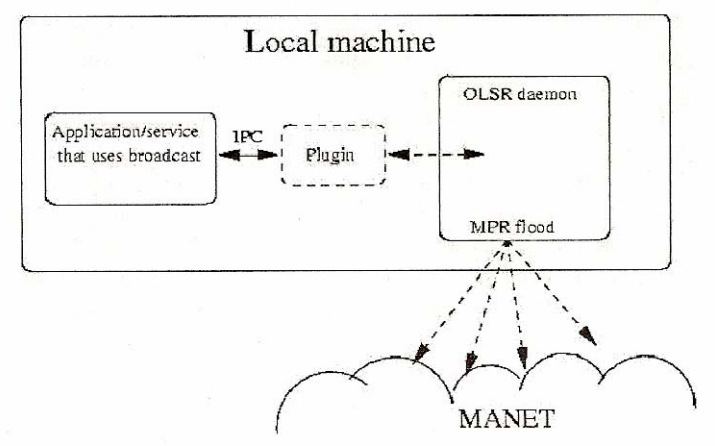

Figure 11. Application using OLSR daemon (From: Tonnesen, Hafslund, and Kure; 2004)

MPRs are selected nodes that forward broadcast messages during the flooding process. The message overhead of the flooding process is reduced substantially compared because the number of control messages flooded by the MPR into the network is minimized, since it is only uses nodes elected as MPRs that generate link state information (Tonnesen, Hafslund, and Kure; 2004). A MPR node may also choose to report only links between itself and its MPR selectors, allowing partial link state information to be distributed to the network. This MPR flooding and default forwarding algorithm used in OLSR makes the protocol very interesting to extend because normal MANET routing suffers from lack of broadcast solutions. By letting OLSR carry broadcast traffic, one can provide a broadcast solution that is optimized. The solution is deemed optimized because the OLSR daemon will then work as a flooding relay agent for local applications (Tonnesen, Hafslund, and Kure; 2004). By using this plugin, the edge unit's (DO,

SOF, UAVs, etc.) applications can be used in the ad hoc environment for seamless communications between air, ground, and Tactical Operation Centers (TOC). In addition, OLSR provides a default forwarding algorithm that allows for forwarding of OLSR messages of unknown types. This means that even if only a subset of the nodes in the network actually know how to interpret a certain message-type, all nodes will forward them accordingly. (Tonnesen, Hafslund, and Kure; 2004). Thus, the information would reach its destination even if one of the relay points could not interpret the data.

MANET solutions forge together edge systems without exposing its routing tables to the larger GIG. This collection of dynamically forming networks exchange information without using any pre-existing fixed network infrastructure (Sun, 2006). And, by connecting these dynamic segments to the larger GIG, the edge unit's information could traverse to any echelon of the DoD C2 infrastructure. There are a bunch of management and routing reasons why this is a good idea. However, the main idea is to enhance the military's Joint C2. MANET eliminates single points of failure by adding alternative routes and deliberately creating routing loops. This communication method for mobile nodes creates greater flexibility and lets initiative stay with our edge units. The edge unit with this mobile communications capability could operate from a Common Operational Picture (COP) and keep the command chain orientated to their actions.

However, not all this capability is without its issues. The core problem with MANETs is that the routing tables constantly change. Due to this volatility, the bandwidth costs and complexity need to be masked within its boundaries. If not masked within the boundary, these detrimental actions cause mayhem in the network. The mayhem is that all routing information protocols, whether conventional autonomous system protocols or development MANET protocols, require some of the network capacity to communicate their routing information from router to router. In spite of this, the MANET protocols require more capacity. Furthermore, proactive MANET protocols like Optimized Link State Routing (OLSR) require capacity for updates regardless of whether actual

content traffic needs a particular link. This “routing situational awareness” must be balanced against overall capacity needs.

D. CONCLUSION

A key aspect of future Joint communication is that MANET enables distributed nodes in the edge environment to communicate between networks in the router layer. This operational ability could decrease the time it takes for coordination between the service components. In a point-to-point, LOS standard military network, integrating 150 nodes into a single network could take 15 minutes, and adding an incremental node could almost take a minute (SAB-TR-05-03, 2005). However, since MANET nodes connect at the Network layer, the nodes could extend our ability to communicate in a distributed manner. This distributed communication would allow independent movement, but leave SOF or DO units with the tacit knowledge that their units are connected to their command structure. The connection of edge units and the command centers is achieved based on Metcalfe’s Law. Metcalfe’s Law observes that although the cost of deploying a network increases linearly with the number of nodes in the network, the potential value of a network increases (scales) as a function of the square of the number of nodes that are connected by the network (Alberts, Garstka, and Stein; 2000). In simpler terms, the value or effectiveness of the network increases exponentially due to fact that each air or ground node added to the network increases the ability for a successful path to be engaged through the GIG to deliver the information from the starting point to the destination point. For these air and ground nodes ingressing to and egressing from the edge network, Optimized Link State Routing (OLSR) protocol is one of the protocol used to assist in traffic control because it is an optimization protocol for mobile ad hoc networks. Remember, Clausen and Jaquet state,

> OLSR is a proactive routing protocol for mobile ad hoc networks. The denser a network, the more optimization can be achieved. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route packets. OLSR means that communications would be fluid because no additional control traffic is generated in

this situation since routes are maintained for all known destinations at all times (Clausen and Jaquet, 2003).

The distributed nodes would have their connections focused by OLSR protocol, and it provides optimal routes in terms of number of hops (Clausen and Jaquet, 2003). The importance of the protocol being suitable for large and dense network is that the sharing of battlespace information and the speed of interaction between those nodes in that battlespace should improve C2 coordination and decrease the amount time to Observe, Orientate, Decide, and Act (OODA) against the enemy. See Figure 12.

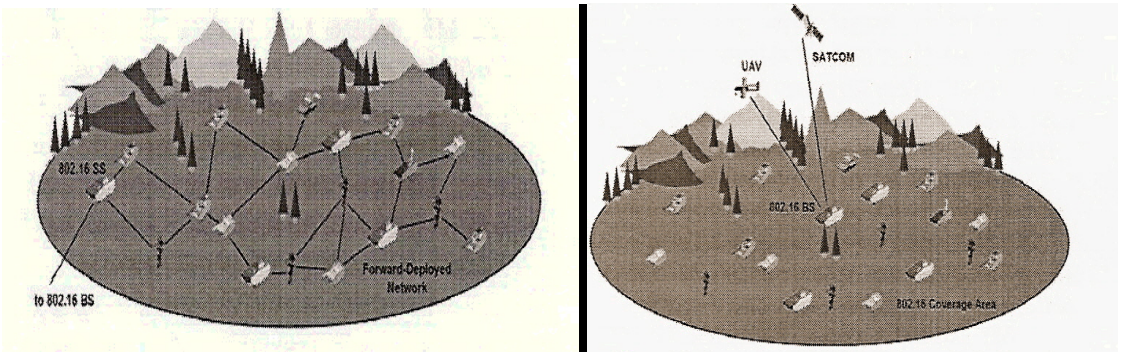

Figure 12. Forward Deployed network connectivity (From: Burbank and Kasch, 2006)

These illustrations portray the possible connectivity for the forward deployed network using MANET technology. And, the protocol would enable ground and air nodes to extend a communications cloud, like the depicted UAV, Satellite, or ground nodes.

In conclusion, the source of potential value for these technologies is the interactions between the nodes. For every "N" node in a network, there are "N-1" potential interactions between the nodes. Therefore, in a network of "N" nodes, the total number of potential value creating interactions are: N x (N-1), or N2-N (Alberts, Garstka, and Stein; 2000). Therefore, for C2 among DO, JCAS, and Joint Fires, these interactions by use of MANETs can provide a maneuverable, auto-configuring, and self-aware capability for Sense, Decide, and Act nodes as they enter and operate in a BLOS area of responsibility (AOR) at the tactical edge environment.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. MESH NETWORK

A. INTRODUCTION

Army, Navy, Air Force, and Marines envision dispersing superbly-trained and equipped tactical units across the battlespace that are connected via an over-the-horizon, on-the-move (OTH/OM) C2 networks that are supported by highly responsive JCAS and Joint Fire (Gilman, 2006). Mesh networking can provide that kind of connectivity.

B. DEFINITION

A Mesh network is defined as a wireless nodes connecting within a network segment at the Medium Access Control (MAC) layer. Mesh end systems communicate by broadcasting their information to the network. Each node can connect directly or indirectly with any other node in the network, and the network offers high reliability since there are many paths through the network from one node to another (Osborne, 2005). Figure 13 is an illustration of a Mesh network.

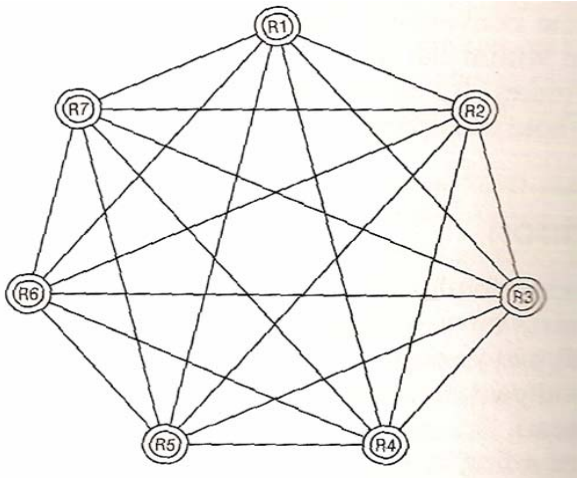

Figure 13. MESH Network (From: Perlman, 1992).

This illustrated Mesh network is precipitated by bridging and the broadcasting of information within the network segment. MAC addresses of each node within the Mesh environment communicate in a PMP or broadcast (Mesh mode) dissemination method.

C. ANALYSIS

Mesh provides networking capability by enabling each subscriber station (SS) to act as bridges by relaying data to nodes that may not have line-of-sight (LOS) to the base station (BS) (Burbank and Kasch, 2006). Within a Mesh network, a system that has a direct connection to backhaul services outside of the Mesh network is termed a BS. All other systems of a Mesh network are termed SS (IEEE Std 802.16a-2003). The MAC layer provides distributed QoS for Mesh. The MAC layer uses non-contention process to handle flow of data. The non-contention process acts as a controlling mechanism to handle the flow of data. The flow of data is controlled by the MAC using contention boundaries (explained in Chapter IV) maintaining a list of all known destination addresses and doing a constant notification process of the activity. Each node of a Mesh network disperses a 48-bit universal MAC address, as defined in the IEEE Std 802.16-2004. The address uniquely defines the node from within the set of all possible vendors and equipment types. This address is used during the network entry process and as part of the authorization process by which the candidate node and the network verify the identity of each other (IEEE Std 802.16-2004). In addition, nodes, by using maintenance windows, connect or disconnect automatically and find a way to link and get the packets transferred to their destination based on the unicast (peer-to-peer) or broadcast (point-to-multi-point (PMP) or Mesh mode). No service or QoS parameters are associated with a link, but each unicast transmission contains service parameters. Traffic classification and flow regulation are performed at the ingress node by the upper-layer portion of the MAC protocol (IEEE Std 802.16-2004).

Mesh networking uses the Layer 1 and Layer 2 areas in data dissemination. In the dissemination of data for Mesh networks, the main difference between the PMP and optional Mesh modes is that in the PMP mode, traffic only occurs between BS and SSs, while in the Mesh mode traffic can be routed through other SSs and can occur directly between the SSs (IEEE Std 802.16-2004), also known as daisy-chaining. In addition, Mesh management of information is determined by algorithms that ensure the best route is chosen at each iteration of transit. One of the algorithms is the Open Shortest Path First (OSPF) protocol. OSPF has no limitation on the hop count, and Link State routing updates are flooded in IP datagrams, and its routing changes are propagated instantaneously (Cisco OSPF Design Guide, 2006). The Link State routing sends status to all SS. The SS uses a graph created from this message traffic to update or build forwarding tables, and the data moves in packet form. Before movement, the packets are embedded in User Datagram Protocol (UDP) datagrams for transmission over the network (Clausen and Jacquet, 2003). UDP provides an end-to-end service that allows an application to send and receive individual messages, each of which travels in separate datagrams (Comer, 2004). In UDP formatting, information can be channeled to all components of a Mesh—demonstrating the ability for decentralized data dissemination. As long as each SS can touch another, the SS accepts a UDP datagram within the mesh architecture.

D. CONCLUSION

In summary, the Mesh networking design offers significant upside for C2 among DO, JCAS, and Joint Fires. Mesh networking refers to the peer-to-peer or point to multipoint, multi-hop data distribution. In this form of communications, the linkage between nodes operates at Layer 1 up to Layer 2 by using PHY/MAC layers. MAC addressing provides self-forming and self-healing by recognizing each node through the MAC protocol. Subsequently, through protocol management at Layer 2, Mesh Sense Decide and Act nodes exchange and

transmit data (voice, video, or text) within a network segment The transmitting of information occurs by each node distributing information to any node in the network segment.

Since the foundation for Joint C2 were discussed in Chapters I, II, and III, and the plausible technical solution was discussed in Chapter IV, V, and VI, Chapter VII supports the hypothesis by walking through the experiments that demonstrated air and ground Joint communications using IEEE 802.16 technology. In addition to experiment overviews, the Chapter VII will also relay findings and make some recommendations.

VIII. EXPERIMENT AND EQUIPMENT OVERVIEW

A. INTRODUCTION

As a Joint Air Force component on the NPS Distributed Operations (DO) team, I postulated that there were benefits offered by using Mesh, MANET, and IEEE 802.16 products in a Joint Networking environment for C2 communications among ground and air assets for JCAS and Joint Fires. Through experimentation, I desired to ascertain whether these technologies could provide a C2 network extension from the GIG to sense, decide, and act (SDA) nodes of a tactical mission. The SDA nodes could coordinate their efforts amongst different service edge units using compatible technology; and, in the same instance, these SDA nodes could also be channeling information directly to the command centers through a Mesh BS connection to the GIG black core entry point. By demonstrating the transfer of data between SDA nodes and the TOC, the experiments will demonstrate that Mesh, MANET, and IEEE 802.16 technologies can improve the interoperability of C2 Constellation Net, FORCEnet, and LandWarNet for a more integrated C2 system for JCAS and Joint Fire support to DO units.

Due to specific, stove-piped, legacy equipment that currently used in the services, the process of coordinating and gaining authorization for JCAS and Joint Fires is time consuming. Each communication relay is point-to-point and does not propagate through C2 network, unless forwarded from the receiving end system. Not only must the CAS request process go through individual LOS links for mission purposes, it must also be coordinated between the commander centers in the same kind of fashion. Furthermore, each of the services has different radio command networks, which require the same kind of efforts at the command echelons. The following process diagrams display the CAS request process and Army/Air Force CAS connectivity.

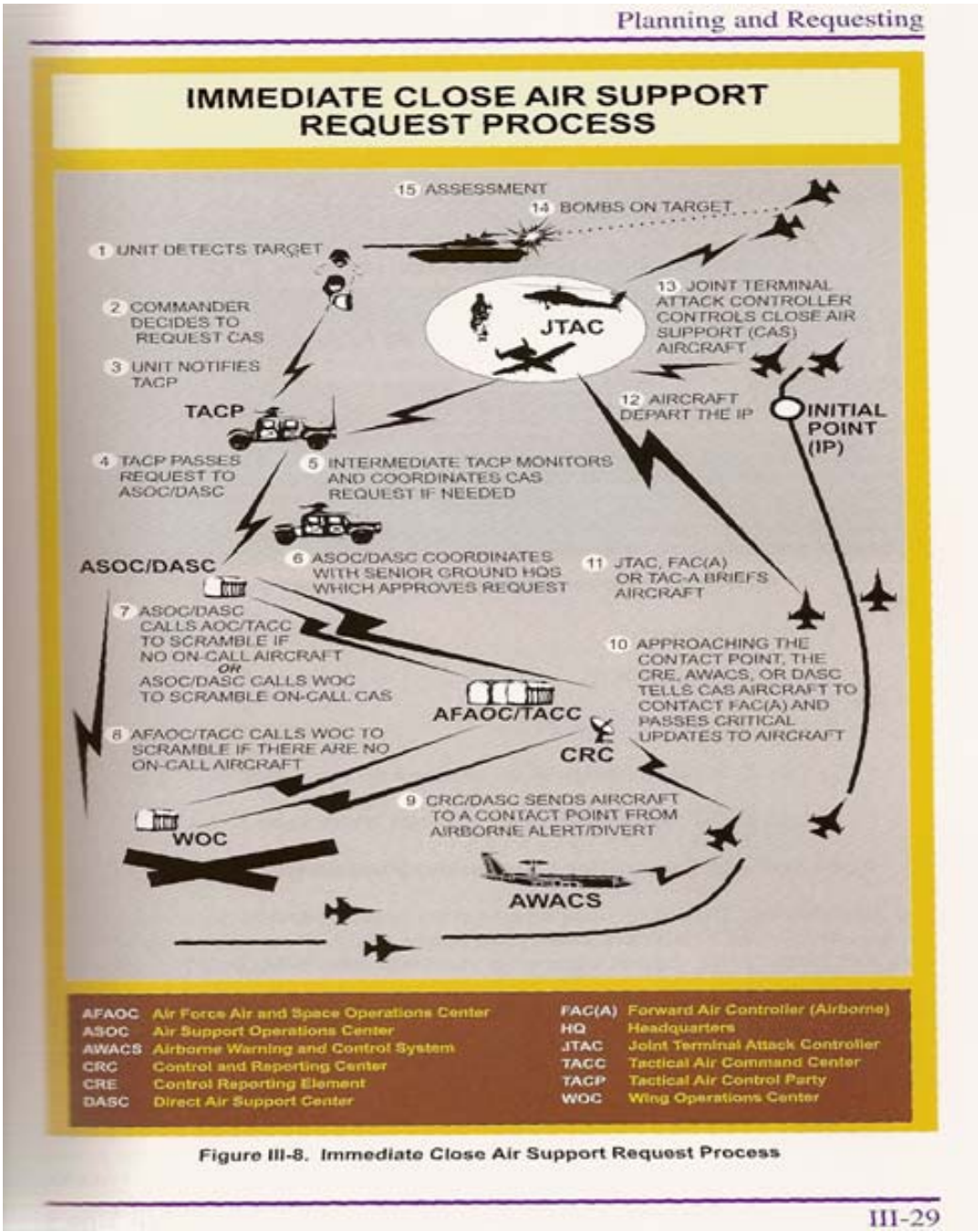

Figure 14. CAS Request Process and Army (From: JP 3-09.3, 2003)

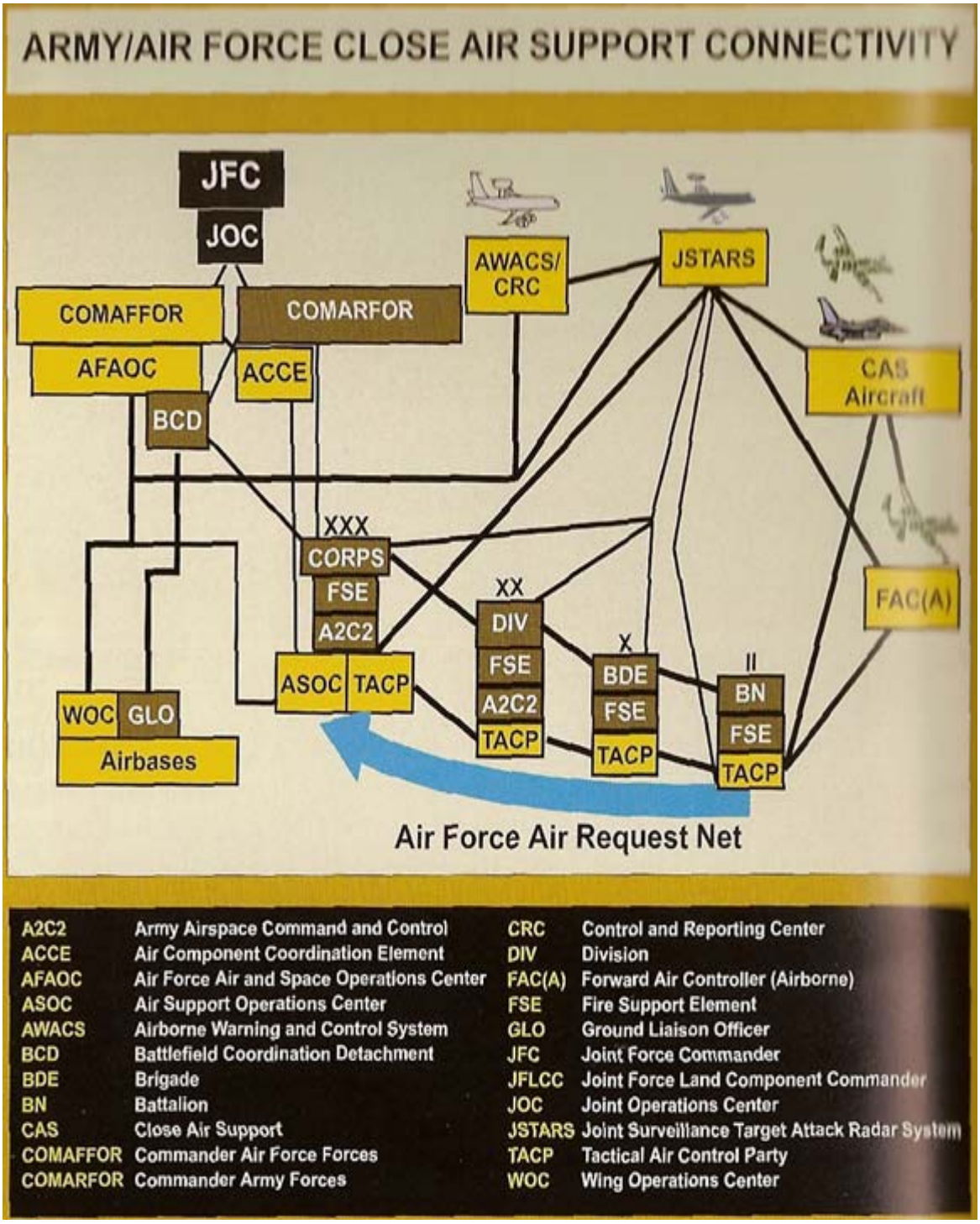

Figure 15. AF CAS Connectivity (From: JP 3-09.3, 2003)

As depicted in the Figure 14 and Figure 15, CAS request process and deconfliction through the Army/AF CAS connectivity involve many diverse and architectural independent platforms that only communicate by point-to-point, LOS HF radio communications. Although the system works, the CAS request process does not use connectionless, interoperable, TCP/IP communications that would provide a virtual connection of all those end systems and create a virtual mesh network. In the CAS request process above, if any one of those links fails, there is no routing mechanism (Layer 3/Network layer) to keep the data moving in a Joint networking way. So, from a networking perspective, there is no actual networking, only a huge amount of direct radio (Layer 1/Physical layer) links between multiple end systems. This disconnection is where my experimentation with mesh nodes becomes a possibility for Joint networking C2.

B. EXPERIMENT OVERVIEW

1. Air to Ground Communications

TNT 06-04 accomplished the task of networking a notional platoon of Marines using TACTICOMPS with ITT Mesh networking cards. Data (voice, video and situational awareness) was passed via the mesh network. This mesh network was pushed to approximately 6km between the farthest mobile node and the Command Operations Center (COC), often Beyond Line of Site (BLOS); but, the signal was often intermittent.

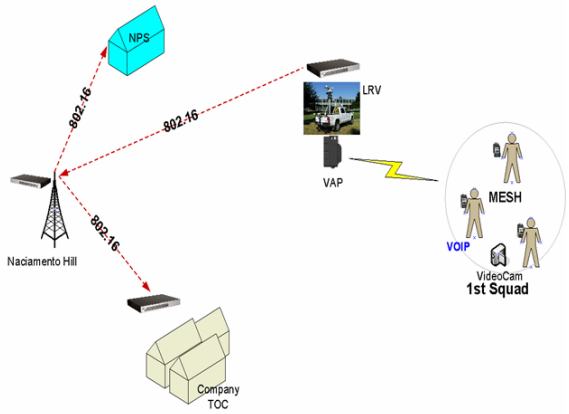

Figure 16. 802.16 Data Transfer from DO unit to NPS (From: Henton and Swick, 2006)

The intent of the experiments was to expand on the work done with TNT 06-04 by incorporating airborne nodes into the network. By utilizing airborne nodes, I hypothesized that the experiments could demonstrate how Mesh, MANET and 802.16-enabled end systems can consistently communicate and be further extended to create a Joint Networking C2 between ground and air nodes for JCAS and Joint Fires network.

1. Balloon as Signal Repeater. The Balloon with a micro mesh router (MMR) was flown at 1000 ft. In this experiment, the balloon acted as a router/repeater (as all nodes in a Mesh network do) in order to extend the connectivity reach of the ground nodes within Line of Sight (LOS) to some components and beyond LOS (BLOS) to other members of the squad/platoon ensuring constant, reliable connectivity to all members of the squad/platoon. With the added altitude of the MMR, the assumption was that all ground components would have clear communications with more nodes in the network at distances greater than those provided by ground based repeaters, thus providing a more reliable routing service, ensuring a more robust network is available to the ground nodes.

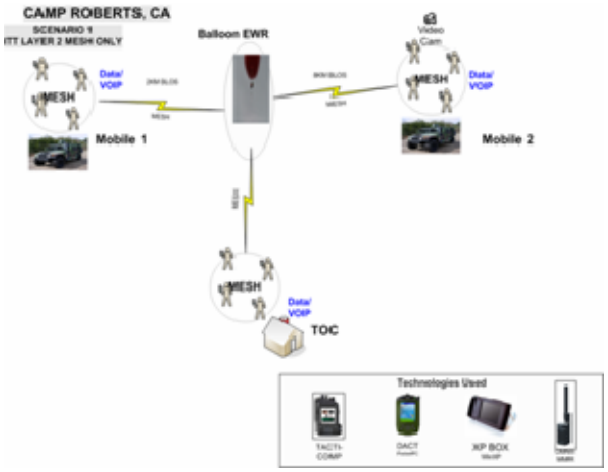

Figure 17. Balloon with an MMR as a static relay point

Success was defined in part by:

- Joining the Mesh Network
- Connecting one or more squads to the COC, BLOS by text, voice and or video (demonstrating all three would be ideal) while the ground node is stationary then in a vehicle

2. Unmanned Aerial System (UAS). The UAS (TERN) aircraft was used to simulate a tactical airborne node for JCAS support to ground operations. The TERN flew at 4000ft, imitating a manned aircraft. For this experiment, the TERN simulated a tactical airborne node capable of conducing Close Air Support (CAS). The TERN loitered and received data files (any data file or a 9-Line CAS) request from any ground node.

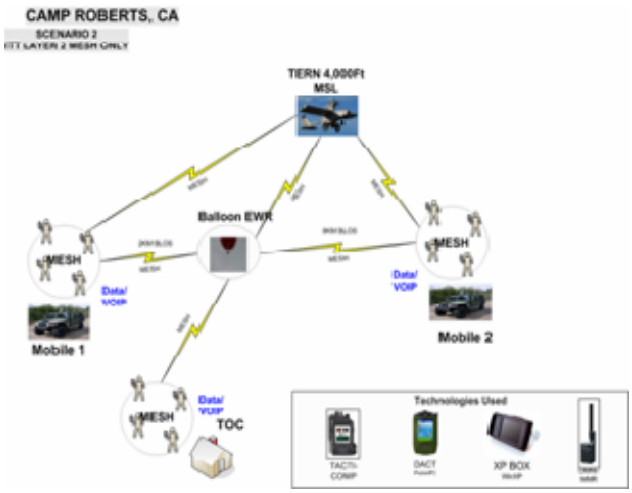

Figure 18. Air to Ground exchange of data (simulation of JCAS request)

Success was defined in part by:

- Joining the mesh network
- Tern receiving data from one or more squads and receiving data from the TOC with text, voice and/or video while the TERN loitered.
- Tern receiving data as one or more ground squads moved.

2. Description of Equipment

a. Inter-4 (Mesh Equipment)

Inter-4 information was obtained from Sierra Nevada Corporation.

Tacticomp 1.5 attached to TERN (UAS) for Air Node

Figure 19. TERN UAS as Simulated CAS Aircraft

Tacticomp™ 1.5

The Inter-4 Tacticomp™ is a Wireless and GPS enabled military hand-held computer designed for field use. The Tacticomp™ offers a unique level of integration in a small, lightweight and rugged design.Its Tactical Modem allows automatic communication through field radios.

Specifications

Processor	32-bit Intel Xscale CPU (400 MHz)
O/S	Windows® CE.netT (4.2)
Memory	96 MB Flash ROM
Working Memory	128 MB
Storage SDRAM	64MB (Battery Backed-up)
Graphics	2-D Accelerator for high speed image manipulation. Video rate: 15-30 frames/sec.
Displays	QVGA, 65K Color Transflective TFT LCD Display, 3.5" Diagonal LED Backlit, Manual Brightness Control, Color Mapping for NVG use (8-bit mode) (Optional VGA CRT Output).
Wireless	LPI, Spread Spectrum, Self-forming and Self-healing Mesh Network Transceiver. Optional: 802 v.11b).
USB	USB mini-A host port, 1 USB mini-B device port. (Optional 2nd USB host port).
GPS	12- channel C/A GPS receiver. Built-in active GPS antenna.
User Input	1 High Resolution Inductive Sensor Stylus and 1 spare Stylus, 4 user buttons, 4 directional and 1 "Enter" Buttons, 2 Screen Brightness Buttons, Power On/Off Button, Recessed "Zeroize" Button.
Power	Standard Battery Pack: Waterproof, Quik-change 50 Whr, Li-Ion Battery Packs - monitors temperature and voltage dynamically to output remaining capacity percentage on LCD display. 110/220VAC Automatic Switching Power Supply and Charger.

Figure 20. Tacticomp 1.5 description (From: Inter-4, 2007)

Virtual Access Point

The Inter-4 Virtual Access Point(VAP)/Backbone(BB) is a wireless access point and video server with back haul capability for dismounted/mounted operations. Its internal multi-channel DSP offers the VAP/BB the ability to broadcast high quality live streaming video from all NTSC video inputs, out to all Mesh-enabled TacticompT devices and to 10BT wired networks.

Specifications

OS	Linux Router
Internal	High Speed Video Encoder/Decoder C/A 12 Channel GPS Receiver (Optional)
Ecryption	256-bit AES Encryption
Wireless	Ad hoc Mesh Tranceiver Card L3, Output 250mw, 2.xxx Transceiver
Power	High Gain, Vehicle-mounted, Omni-directional Antenna
Optional Accessories	Direction Sensing Antenna, Toc Antenna mounted and RF Cable
Case/Weight	10" x 8" x 7" , 10 lbs
Case	Composite Housing/Access Port, TPR Overmold
Seals	O-ring Sealed on Case
Anti-tamper Design	Double 90 tongue and groove case design, with anti-tamper fasteners
Enviromental Spec	Storage Temperature: -26 to 160 °F, Operating Temperature: -22 to 160 °F, Operating Humidity Range: 5% to 100% Non-operational, Operating Humidity Range: 10% to 100%, Operational Vibration: MIL-STD-810F, Method 514.5, Shock/Drop: MIL-STD-810F, Method 516.5, Sand & Dust: MIL-STD-810F, Method 510.4, Rain: MIL-STD-810F, Method 506.4, Salt Fog: MIL-STD-810F, Method 509.4, Altitude: MIL-STD-810F, Method 500.4, Fungus Resistance: External Surfaces, Fungus Resistant, EMI/EMC: Designed to meet MIL-STD-461E, Waterproof: 1 meter.

Figure 21. Virtual Access Point: entry to GIG (From: Inter-4, 2007)

Tacticomp™ 6

The Inter-4 Tacticomp™ is a Wireless and GPS enabled military hand-held computer designed for field use. The Tacticomp™ offers a unique level of integration in a small, lightweight and rugged design.Its Tactical Modem allows automatic communication through field radios.

Specifications

Processor	1.8 GHz Intel® Pentium® M Processor.
O/S	Windows® 2K, XP, Linux or Solaris™
Memory	Up to 1GB SDRAM
Flash	User configurable, 1 type 2 Compact Flash slot.
Graphics	3-D Accelerator for high speed image manipulation. OpenGL compliant.
Displays	8.4" SVGA (800x600), Color TFT LCD Display, Backlit, Manual Brightness Control, Color Mapping for NVG use.
Wireless	LPI, Spread Spectrum, Self-forming and Self-healing Mesh Network Transceiver. Optional: 802 v.11b).
USB	4 USB 2.0 host ports (480 mbps).
GPS	12-channel C/A GPS receiver. Built-in active GPS antenna.
User Input	1 High Resolution Inductive Sensor Stylus and 1 spare Stylus, 4 user buttons, 4 directional and 1 "Enter" Buttons, 2 Screen Brightness Buttons, Power On/Off Button, Recessed "Zeroize" Button.
Power	50Whr Extended Life Li-Ion Battery Pack-monitors temp and current drain to output remaining capacity percentage on LCD Screen. 110/220 VAC Switching Power Supply and Charger.
Battery Protection	Over charge, over discharge, over current, over temperature protection.

Figure 22. Tacticomp 6 description (From: Inter-4, 2007)

Tacticomp™ 5

The Inter-4 Tacticomp™ is a Wireless and GPS enabled military hand-held computer designed for field use. The Tacticomp™ computers offers a unique level of integration in a small, lightweight and rugged design.Its Tactical Modem allows automatic communication through field radios.

Preliminary Specifications (Prototype)

Processor	1.0 GHz Intel® Pentium® M Processor.
O/S	Windows® 2K, XP, Linux or Solaris™
Memory	Up to 1GB DDR SDRAM
Flash	user configurable
Graphics	Intel® Graphics Accelerator for image manipulation. OpenGL compliant.
Displays	6.4" SVGA (800x600), Color TFT LCD Display, Backlit, Manual Brightness Control, Color Mapping for NVG use.
Wireless	LPI, Spread Spectrum, Self-forming and Self-healing Mesh Network Transceiver. Optional: 802 v.11b).
USB	1 USB mini-a host port, 1 USB mini-B device port.(Optional 2nd USB host port).
GPS	12-channel C/A GPS receiver. Built-in active GPS antenna.
User Input	1 High Resolution Inductive Sensor Stylus and 1 spare Stylus, 4 user buttons, 4 directional and 1 "Enter" Buttons, 2 Screen Brightness Buttons, Power On/Off Button, Recessed "Zeroize" Button.
Power	50Whr Extended Life Li-Ion Battery Pack-monitors temp and current drain to output remaining capacity percentage on LCD Screen. 110/220 VAC Switching Power Supply and Charger.
Battery Protection	Over charge, over discharge, over current, over temperature protection.
Battery	Replaces Battery Packs, plugs into the AC/DC Adapter (eliminating need for batteries in prolonged stationary usage).

Figure 23. Tacticomp 5 description (From: Inter-4, 2007)

Omni-directional Micro Mesh Router

The Inter-4 Omni-directional Micro Mesh Routers (ODMMR) is a wireless device that transmits data up to 12 miles. The ODMMR links a squad to Situation Awareness, Real-time VoIP and Video.

Specifications

OS	Ad hoc, Self-forming and Self-healing Mesh Transceiver.
Internal	Heavy Duty Battery Pack: Waterproof, 50 Whr, Li-Ion Battery Packs.
Case/Weight	Micro Mesh Router : 4.5" x 9" x 3" Antenna: 26" x .75" x .75"
Wireless	Composite Housing/Access Port, TPR Overmold.
Power	O-ring seals on Case.
Optional Accessories	Double 90° tongue and groove case design, with anti-tamper fasteners.
Enviromental Spec	Storage Temperature: -26 to 160 °F, Operating Temperature: -22 to 160 °F, Operating Humidity Range: 5% to 100% Non-operational, Operating Humidity Range: 10% to 100%, Operational Vibration: MIL-STD-810F, Method 514.5, Shock/Drop: MIL-STD-810F, Method 516.5, Sand & Dust: MIL-STD-810F, Method 510.4, Rain: MIL-STD-810F, Method 506.4, Salt Fog: MIL-STD-810F, Method 509.4, Altitude: MIL-STD-810F, Method 500.4, Fungus Resistance: External Surfaces, Fungus Resistant, EMI/EMC: Designed to meet MIL-STD-461E, Waterproof: 1 meter.

Figure 24. Omni-directional Micro Mesh Router (MMR) (From: Inter-4, 2007)

Directional Micro Mesh Router

The Inter-4 Directional Micro Mesh Routers (DMMR) is a wireless device that transmits data up to 30 miles. The DMMR links a squad to Situation Awareness, Real-time VoIP and Video.

Specifications

OS	Ad hoc, Self-forming and Self-healing Mesh Transceiver.
Internal	Heavy Duty Battery Pack: Waterproof, 50 Whr, Li-Ion Battery Packs.
Case/Weight	Micro Mesh Router : 4.5" x 9" x 3" Antenna: 11.6" x 11.2 " x .75"
Wireless	Composite Housing/Access Port, TPR Overmold.
Power	O-ring seals on Case.
Optional Accessories	Double 90° tongue and groove case design, with anti-tamper fasteners.
Enviromental Spec	Storage Temperature: -26 to 160 °F, Operating Temperature: -22 to 160 °F, Operating Humidity Range: 5% to 100% Non-operational, Operating Humidity Range: 10% to 100%, Operational Vibration: MIL-STD-810F, Method 514.5, Shock/Drop: MIL-STD-810F, Method 516.5, Sand & Dust: MIL-STD-810F, Method 510.4, Rain: MIL-STD-810F, Method 506.4, Salt Fog: MIL-STD-810F, Method 509.4, Altitude: MIL-STD-810F, Method 500.4, Fungus Resistance: External Surfaces, Fungus Resistant, EMI/EMC: Designed to meet MIL-STD-461E, Waterproof: 1 meter.

Figure 25. Micro Mesh Router (MMR) description (From: Inter-4, 2007)

b. Redline (802.16 Equipment)

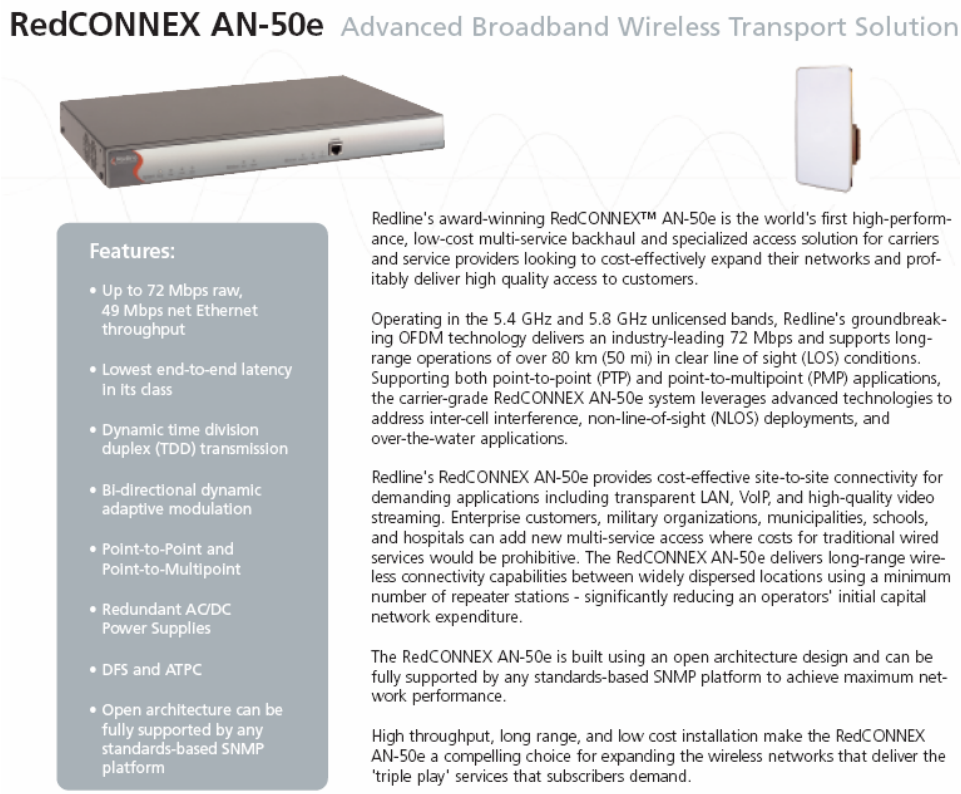

Figure 26. Redline AN-50E (From: www.redlinecommunications.com, 2007)

The model AN-50e (see Figure 26) is a pre-IEEE 802.16 implementation that contains most of the features in the standard. And, it constitutes a routable network. In the case of this gear, Ethernet-frames pass from IEEE 802.16 nodes to other nodes. These nodes patch into conventional bridges and routers for forwarding across the inter-network. Also, the socket on the front panel of the illustration is an Ethernet-socket. Hence, the AN 50s implement the essentials of the IEEE 802.16 scheduling, because the MAC layer:

- Provides Ethernet-numbering and support to point-to-multipoint, which supports for multicasting.
- Contains security features, but the requirements were undefined and immature at this first implementation.

- Simple Network Management Protocol (SNMP) Management Information Base (MIB) is certainly there, but also immature and untested.

C. SUMMARY OF EXPERIMENT FOR 07-01

1. Scope of Experiment

For testing the thesis, an AB, AB testing methodology was used. In the experimentation, three positions for simulated DO squads were established and a position for the TOC was obtained. Then, the testing attempted a BLOS data communication exchange, A Test. The A Test of connectivity and throughput provided the baseline for the experiment. Squad units were positioned in 354411N/1204609W and 354340N/1209647W gulley locations, and at 354711N/1204418W barracks area. From these locations, these squad units attempted, but were unable to exchange data (voice, video, or files) to one another and/or the TOC. So, the A Test baseline established that communications BLOS was one of non-connectivity. After the baseline was established, my experimentation focused on the two experiments of adding air nodes, B Tests. The B Tests added:

- a static balloon with an Omni-directional MMR
- TERN (with Tacticomp) and Rascal (with Highpoint Card).

In the experiments, the static balloon with the Micro Mesh Router (MMR) established a Mesh network between the ground units BLOS, and the UAS. The experiment demonstrated that real-time exchange of data between air and ground edge units and the TOC could be done (simulating JCAS and Joint Fires coordination possibilities with Mesh, MANET, and IEEE 802.16 technologies). In addition, the B Tests provided continuous connectivity between the edge units. Moreover, the squads were be able to move and transmit data to the TERN (with a Tacticomp 1.5) to test MANET capabilities and the affect Doppler has on data transfer from moving ground components to moving air node.

Therefore, in summary, the AB, AB testing furnished results that demonstrate data exchange is achievable in real-time between air and ground nodes and TOC. The following is a list of mac addresses and the names associated with the air and ground nodes experiment.

- 00-05-12-DA-88-50 Balloon
- 00-05-12-DA-A2-35 Mobile 4
- 00-05-12-DA-89-3F Mobile 2
- 00-05-12-DA-9E-85 Mobile 1
- 00-05-12-DA-A1-D6 Highpoint 1
- 00-05-12-DA-9E-76 Highpoint 2
- 00-05-12-DA-A2-5F Air 2 (TERN)
- 00-05-12-DA-A2-87 Mobile 5
- 00-05-12-DA-8F-4F Nemesis
- 00-05-12-DA-AC-40 Rascal

Consequently, adding to the successful 06-04 experiments by Henton and Swick, 2004, these experiments also demonstrated that transmission of data across the network from the TOC to the other C2 components of the Army/Air Force CAS could occur through the GIG. Thus, the experiment demonstrated (although in limited fashion) that Joint networking C2 between DO, JCAS, and Joint Fires is possible, and the ad hoc connection from Air/Ground to TOC showed that the information could be sent simultaneously to any of the command centers connected to the GIG.

2. Results of Experiment

1. Ground to Ground BLOS communication

- Demonstrated that adding a Micro Mesh Router (MMR) to a balloon as a static relay point could establish Mesh network BLOS and extend Mesh communications up to 8 kilometers between mobile units that were not able to communicate (real-time voice, data (video), and files).

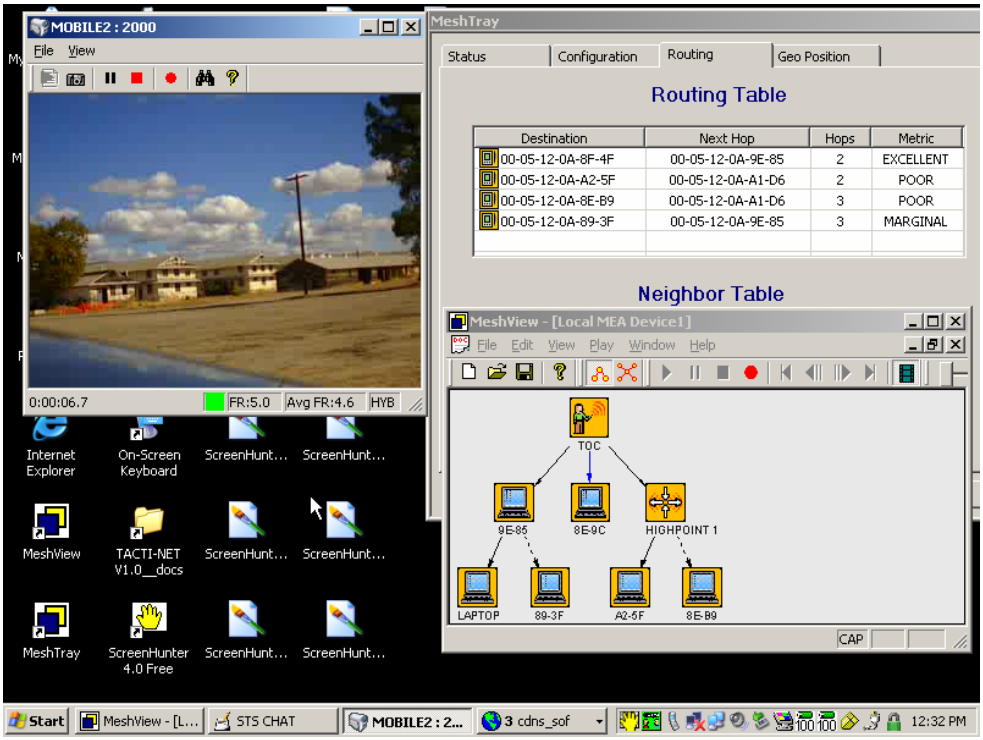

Figure 27. Mesh network from Barracks to TOC established with MMR

2. Air to Ground communication

- Demonstrated that data could be over a mesh network to airborne and ground nodes, simultaneously
- Air node (TERN) received data at 4,000ft in the simulation of aircraft loitering for CAS support and receiving a 9-line CAS message
- Demonstrated that video could be streamed real-time to separate squads and communicated to TOC and COC for real-time assessment and relaying of orders without the information being corrupted

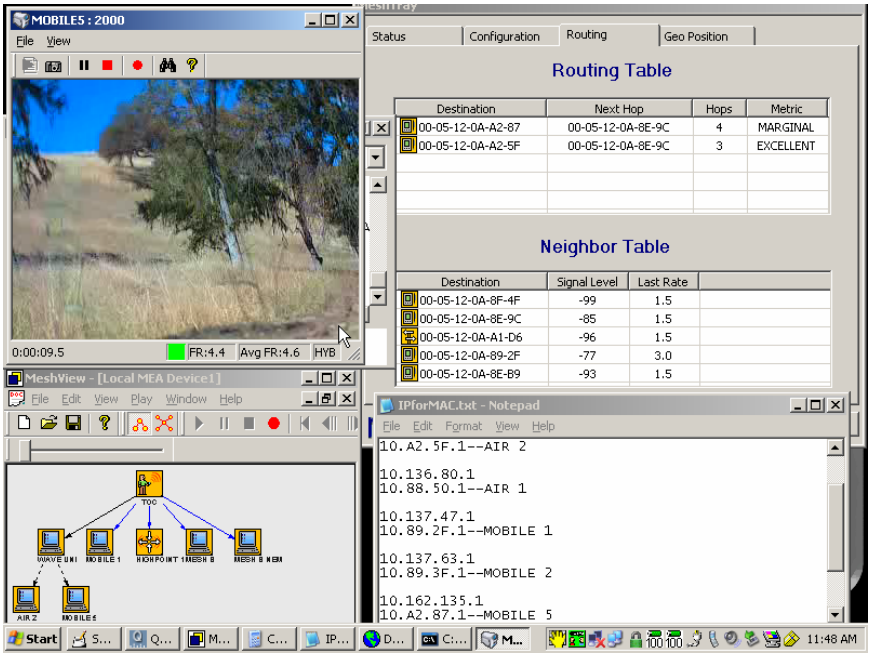

Figure 28. Data to Air and Ground

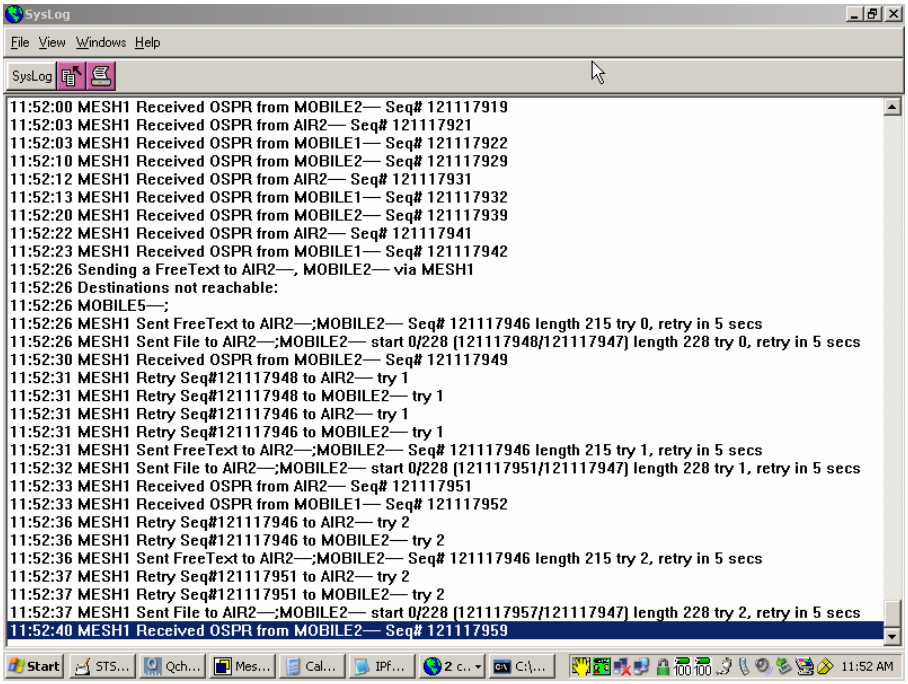

Figure 29. Syslog of TERN and DO units receiving data

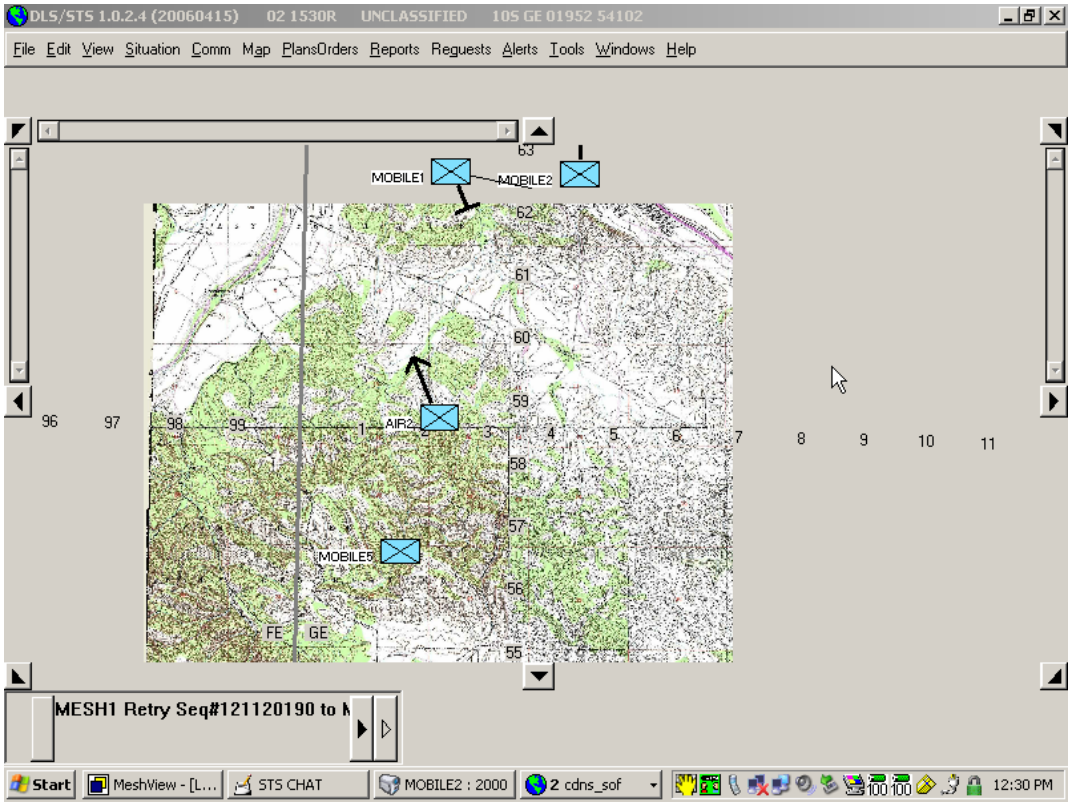

Figure 30. Location of DO units and Air node

3. Real-time transfer of data uncorrupted

- Demonstrated that data (Biometric or 9-line CAS) could be sent uncorrupted by means of AES encryption on a COTS product over a mesh network.
- Biometrics data files from TOC to an entry control point BLOS, so that the Marines could coordinate real-time with the TOC or COC (validated at West Virginia Biometric Fusion Center).
- Biometrics data files were sent to BLOS to SOF , uncorrupted and authenticated (validated at West Virginia Biometric Fusion Center).
- Capability for data transfer over to COC, or other Army and Air Force centers IEEE 802.16 incorporates results from 06-04 DO experiments.

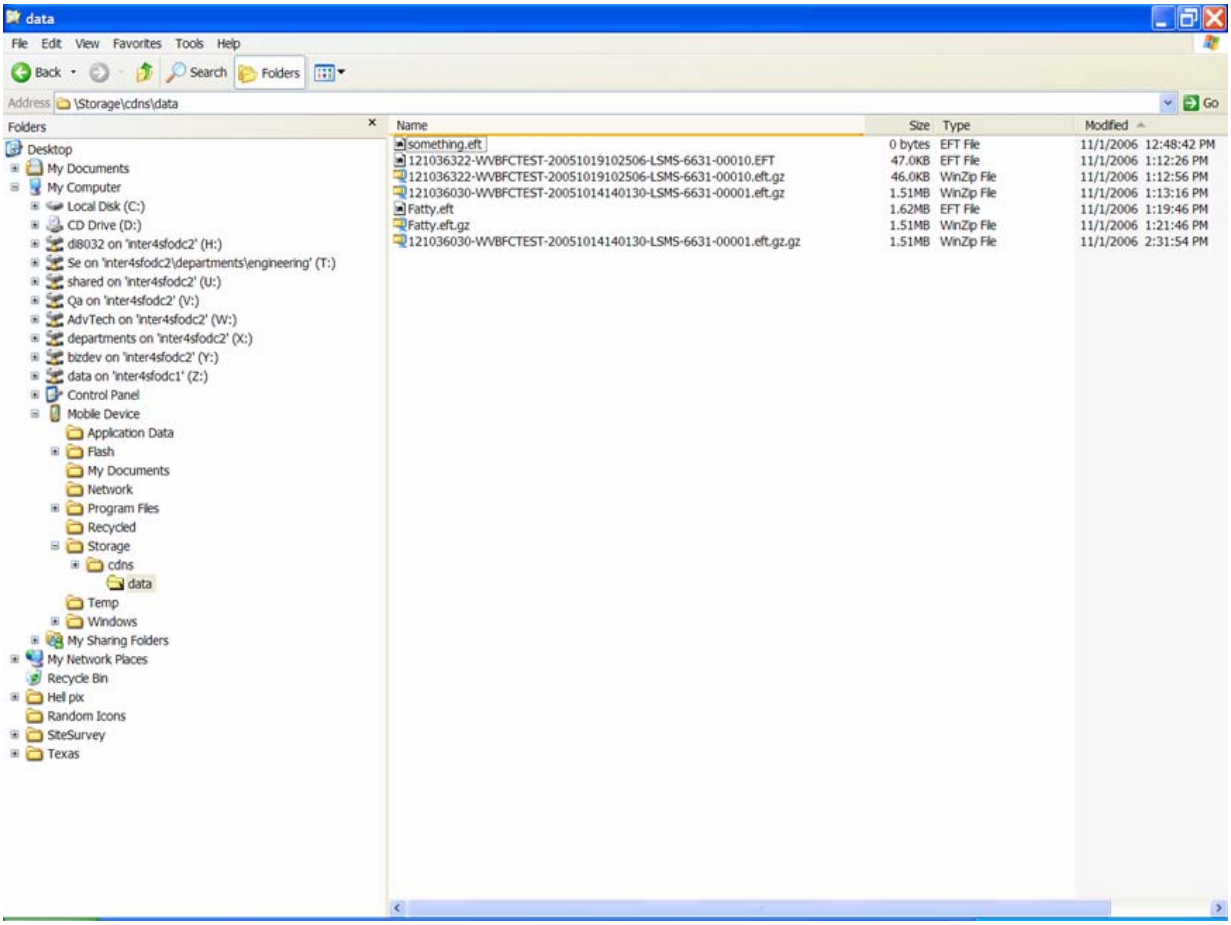

Figure 31. Uncorrupted Biometric Files (Authenticated by Biometrics Fusion Center)

4. Selection of best path

- Demonstrated Mesh traffic would use OSPF routing and dynamic routing on strength of signal

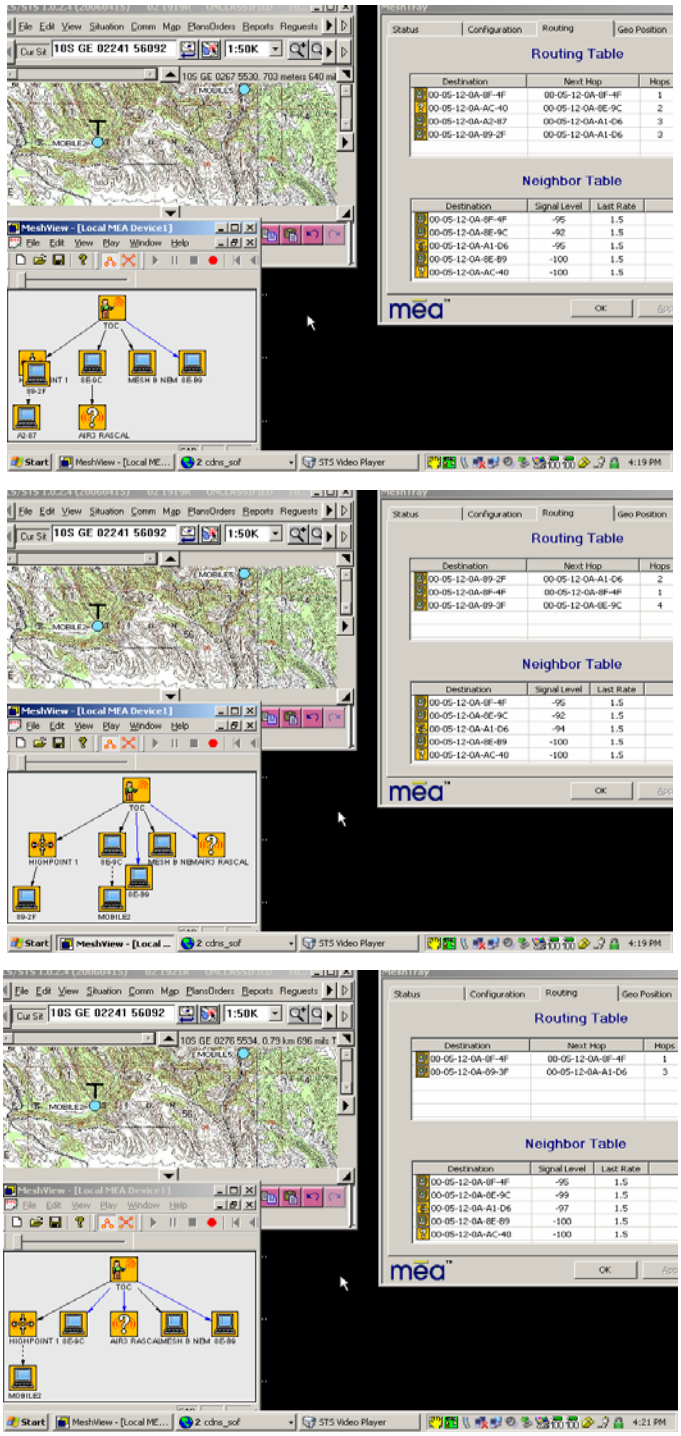

Figure 32. 3 Pictorials showing dynamic routing, in sequential order

D. CONCLUSION

From the use of qualitative AB, AB testing methodology, the experiments demonstrated that Mesh, MANET, and IEEE 802.16 technology could improve

Joint Networking C2 at the edge environment, BLOS. By using a balloon at 1000ft, with a MMR and an omni-directional antenna, the Mesh network extended to over 8km. DO squads in disparate locations communicated, via VOIP, chat, exchange of data files, and video feeds. Moreover, all squads communicated with each other and to the TOC. In addition, by using the TERN and Rascal, the experiments demonstrated that data could be exchanged real-time between air and ground nodes. The TERN at 4000ft was a valuable asset in the simulation of an aircraft in a CAS holding pattern. Although it was only moving at 60 to 75 knots, it provided a successful real-time air node for data exchange between air and ground node using COTS equipment, and demonstrated a possible solution. Additionally, the use of the Rascal with the mesh card showed that data paths change dynamically based on OSPF protocol and signal strength of the nodes in the spanning tree. These dynamic changes and self-healing attributes at routing continue to illuminate the importance of using the Mesh, MANET, and IEEE 802.16 technologies to ensure delivery of information to all echelons of the military structure in a more timely manner that capitalizes on GIG-BE's compatibility to transmit data according IEEE OSI standards. Lastly, with there being security concerns with the exchange of data using these technologies, the experiments demonstrated that data integrity and authenticity are maintainable because biometrics data files were sent uncorrupted. This fact was validated by the Biometrics Fusion Center in West Virginia.

Overall, these experiments showed that Joint forces can communicate, collaborate and share a common operational picture (COP) composed of voice and data as well as imagery. The forward deployed marine, soldier, or airman will continue to be our main forward sensor. By using ad hoc technology to increase our interoperability between airborne nodes, ground nodes, and command centers, our Joint C2 operations can improve and allow our SDA forces to act upon a common situational awareness and real-time authorization from higher level decision makers.

IX. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

IEEE 802.16 is compatible with the connectionless OSI constructed GIG because its foundation is based on the IEEE 802.3. Therefore, the DoD only needs to better define its requirement, so COTS vendors could make modifications specifically designed to meet DoD requirements. This redefining and scoping of requirements encourages competition based on the IEEE standards. This open competition would increase availability of products to meet military interoperability requirements for Joint communication, and it would allow future end-systems to be compatible to the current IPV4 and upcoming IPV6 GIG enhancements by DISA.

This thesis reviewed the proposed DO communications architecture being pursued by Marine Corps, and it referenced the C2 Constellation Net, FORCEnet and LandWarNet concepts being considered by the Air Force, Navy, and Army, respectively. The review of the concepts and architectures was to ensure that the hypothesis of improving Joint C2 among DO, JCAS and Joint Fires was possible through IEEE 802.16 was plausible. The review of converging architectures illuminated that Joint Networking C2 using Mesh and MANET could enhance our separated services abilities to operate with greater speed of communications to the edge units of our military structure and act as a quick stand up communications medium for emergency situations. Hence, this thesis' research drive was to determine the depth and extent of how these technologies could solve the interoperability problems surrounding integrated Joint C2 capabilities.

By using stable, routable networks based on compliant IEEE OSI model technologies, the services could capitalize on the investment done by DISA in the GIG-BE. In TNT 06-04, DO units transmitted video from camera to other members of the mesh, including to NPS via Tactical Operations Center (TOC) by using an IEEE 802.16 tie-in (Henton and Swick, 2004). From these previous DO

experiments, this thesis leveraged its experiments on air nodes enhancing communication exchange between air and ground units. It was also attempting to transmit that information back through the GIG. In experiments, the thesis:

- Demonstrated that a Mesh and MANET are extendable BLOS without intermittent communication when a balloon with an EWR attached is raised to 1000ft.
- Demonstrated that a Mesh and MANET could cover over 8 kilometers by adding air components.
- Demonstrated a real-time data exchanged between an airborne node at 4000 ft. and ground nodes (simulating 9-line for JCAS and Joint Fires).
- Demonstrated sending Biometric data files encrypted and uncorrupted to a simulated entry control point over 8 kilometers (verified at Biometrics Fusion Center).

Overall, this thesis fused the DO concept to the proposed doctrine of Joint C2 through the employment of Mesh and MANET COTS equipment. The thesis experiments demonstrated that connecting small, distributed units to other service end systems for JCAS and Joint Fires is possible with more research and development. Moreover, the thesis experiments illustrate that IEEE 802.16 products connect to other internet infrastructure, such as the commercial Internet and the Defense Information Switched Network. The simulated DO squads and SOF units changed positions throughout the experiments and verified that ground to ground communication could be enhanced with a static relay being instituted by an omni-directional router attached to a balloon. And, the second experiment demonstrated that ground units could exchange data with moving air components that have mesh devices attached. In addition, both of the experiments demonstrate data exchange in real-time between air/ground for possible coordination of targeting information. By bridging the gaps with COTS equipment, the DoD could utilize a more accessible and less expensive logistics supply than those items developed within the DoD. In addition, the contentionless service of IEEE 802.16 technologies are already primed to provide availability, authenticity, security, QoS control, and self-healing, self-forming capabilities, due to the present drives of the commercial market.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

Future experiments of air to ground communications should include a targeting and ranging system that Marines use in coordination with CAS. The system needs to be tested for compatibility to Mesh and MANET enabled end systems. The test should focus on whether the system can connect to an airborne MANET and disseminate tactical information to other DO units, as well as exchange that data back through BS to the GIG for coordination with other services components for JCAS and Joint Fires. In addition, more research and experimentation needs to be done in the TNT environment with manned-aircraft to test the maximum operational capabilities of MANET enabled air nodes and ground units.

In summary, commercial information technology enables convergence of technologies for voice and data services. Furthermore, this technology allows the network to maintain stability, enables bandwidth efficiency, and provides QoS. The technologies that emerge from the commercial sector, if augmented with specialized information technologies developed by the DoD, such as high encryption, low-probability of intercept and detection communications, and specialized intelligent agents, could provide the brick and mortar for our GIG (Alberts, Garstka, and Stein, 2000). Currently, the progressions being made in private sector are creating opportunities for the DoD to capitalize on the technology revolution surrounding distributed systems computing. Some of the technologies that assist in creating a distributed, beyond line of sight, high bandwidth environment for voice and data should be exploited. Since Mesh and MANET with other emerging distributed hardware/software solutions are being reified, proliferation and usage would drive down the price of enacting these technologies and enhance the DoD's ability to deploy standardized communications fly away kits in adverse theaters quickly and cost effectively.

In their paper "Designing Wireless Radio Access Networks for Third Generation Cellular Networks" Bu, Chan, and Ramjee state:

> Ability to house and deploy standardized communication packages will set the stage for U.S. to be able to provide C2 communications services in austere, non-infrastructure regions. IEEE 802.16 operates in both line-of-sight and non-line-of-sight modes, thus allowing deployments in regions where there is no direct line-of-sight. In addition, IEEE has addressed the reliability issues of failure of links or nodes by designing algorithms to create topologies that can handle single failures effectively (Bu, Chan, and Ramjee, 2005).

Moreover, analysis in Chapters IV and V walk through the IEEE 802.16 Medium Access Control (MAC) layer protocol and shows that, in addition to being network routable, it has a stable, non-contention Medium Access Controller. This stable and non-contentious controller makes IEEE 802.16 greatly superior to other radio data technologies such as Mil-Std-188-220 and IEEE 802.11. In addition, IEEE 802.16 technology enables the DoD components to overcome single failure effectively because the ad hoc network would operate in a connectionless environment between WAN segments in a global environment, while Mesh enables linkage with edge units within a particular network segment. Each of the capabilities creates a level of assurance transmission integrity can be maintained and that mission data will be delivered. And, because the security is configured into communication within the MAC layer, as well, the data integrity issues can be addressed independently. Overall, by using a mixture of IEEE 802.16 technology, DoD could eliminate single points of failure at the tactical edge and provide a means for units to coordinate seamlessly and effectively among DO, JCAS, and Joint Fires.

LIST OF REFERENCES

Adams, Charlotte. "Network Centric, Rush to Connect." Defense Daily Network: Aviation Today 6 September. 2004. <http://www.aviationtoday.com>.

Alberts, David S.; Garstka, John J.; and Stein, F. P. Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition. February. 2000.

Bu, T.; Chan, M. C.; and Ramjee, R. "Designing Wireless Radio Access Networks for Third Generation Cellular Networks." IEEE. 2005.

Buddenberg, Rex. "Objective, Architecture and Strategy for Network Centric: A Perspective on Mobile Communication's." Naval Postgraduate School December. 2005.

Burbank, Jack L and Kasch, William T. "IEEE 802.16 Broadband Wireless Technology and Its application to the military problem space." The Johns Hopkins University Applied Physics Laboratory (JHU/APL). 2006.

C4ISR Flight Plan; USAF/XI, Headquarters United States Air Force.

Cisco: Quality of Service. 5 October. 2006. <http://www.cisco.com>.

Clausen T. and Jacquet P. Optimized Link State Routing Protocol (OLSR): RFC 3626. The Internet Society October. 2003.

Coakley, Thomas P. Command and Control for War and Peace. Washington, National Defense University, 1991.

Comer, Douglas E. Computer Networks and Internets with Internet Application, 4th Edition. West Lafayette: Pearson Education, 2004.

Deitel, H. M. Operation Systems, 2nd Edition. Addison-Wesley Publishing Company, Inc. February. 1990.

Director for Strategic Plans and Policy, J5, Strategy Division. Joint Vision 2020. U S Government Printing Office June. 2005.

Draves, Richard; Padhye, Jitendra; and Zill, Brian. "Routing in Multi-Radio, Multi-hop Wireless Mesh Networks." Microsoft Research MobiCom'04 September. 2004.

Eklund, Carl, Marks Roger B., Stanwood, Kenneth L., and Wang, Stanley. IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. IEEE Communications Magazine. June. 2002: 98-107.

Engelstad, P.; Tonnesen, A.; Hafslund, A.; and Egeland, G.; “Internet Connectivity for Multi-Homed Proactive Ad Hoc Networks” OLSR Interop and Workshop. 2004.

Fineberg, Victoria. “The Role of IPv6 and MPLS in the GIG Black Core.” Falls Church: DISA-IPv6 Transition Office 2006: 1-6.

Gilman, Brian L. Distributed Operations: Translating Tactical Capabilities into Operational Effects. Naval War College. 13 February 2006.

Godfrey, P. B.; Shenker, Scott; and Stoica, Ion. “Minimizing Churn in Distributed Systems.” U. C. Berkeley, Computer Science Division SIGCOMM’ 06 September. 2006

Green, J. H. The Irwin Handbook of Telecommunications 3rd Edition. Pantel, Inc. 1997.

Hafslund, A.; Tonnesen, A.; Rotvik, R. B.; Andersson, J.; and Kure, O. “Secure Extension to the OLSR protocol.” OLSR Interop and Workshop. 2004.

Hagee, M.W. A Concept for Distributed Operations. Department of the Navy, Headquarters U.S. Marine Corps; April. 2005.

Henton, G. and Swick, J. Extending the Tactical Wireless Internet in Support of USMC Distributed Operations. Naval Postgraduate School September. 2006.

IEEE Amendment to IEEE STD 802.16—Medium Access Control. Computer Society IEEE. 2003.

IEEE Recommended Practice for Local and Metropolitan Area Networks. Computer Society IEEE. 2001.

Inter-4 Equipment Descriptions. Sierra Nevada Corporation. April. 2007. <http://www.sncorp.com>.

Joint Fires Integration and Interoperability Team (JFIT. United States Joint Forces Command February. 2005.

McClelland, Frank M. “Services and Protocols of the Physical Layer.” National Communication System, October. 1982.

Navy League of the United States. “The Challenge of Joint Fire Support Interoperability.” July. 2007.

OSPF Design Guide. CISCO Systems. 11 July. 2006. <http://www.cisco.com>.

Perlman, Radia. Interconnections: Bridges and Routers. Addison-Wesley Publishing Company, Inc. 1992.

Radhakrishnan, S.; Racherla, G.; Sekharan, C.; Roa N.; and Batsell S. "Protocol for Dynamic Ad-Hoc Networks Using Distributed Spanning Trees." Wireless Networks November. 2003.

Redline AN-50E. 15 Apr. 2007. <http://www.redlinecommunications.com>.

Robinson, Terri. "Widespread, wireless broadband heralds a new era of unlimited accessibili." WIMAX TO THE WORLD December. 2005: 29-34.

Roman, Gregory A. The Command and Control Dilemma: When Technology and Organizational Orientation Collide. Air War College Maxwell Paper No. 8. Maxwell AFB Ala. March.1997.

Rose, Marshall T. "Transition and Coexistence Strategies for TCP/IP to OSI." NYSERNet, Inc. July. 1988.

SAB-TR-05-03 Report on Domain Integration. United States Air Force Scientific Advisory Board. : Executive Summary and Annotated Brief. July. 2005.

Self-Organizing Neighborhood Wireless Mesh Networks: Overview. Microsoft. Nov. 2006. <http://www.microsoft.com>.

Service-oriented architecture (SOA) definition. 31 May 2007. <http://www.service-architecture.com>.

Snyder, Frank. M. Command and Control: The Literature and Commentaries. Washington: National Defense University. 1993.

Sun, Jun-Zhao. "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing." Machine Vision and Media Processing Unit, University of Oulu, Finland. 2006.

Tonnesen, A.; Hafslund, A.; and Kure, O. "The UniK-OLSR plugin library." THALES Communications AS and UniK-University Graduate Center OLSR Interop and Workshop. 2004.

Tovar, Edward Lt Col. "USMC Distributed Operation." Advanced Technology Office DARPATECH 9-11 August. 2005: 22-24.

United States Government as presented by Department of Defense. Department of Defense Interface Standard: Digital Message Transfer Device Subsystems. DoD MIL-STD-188-220C. May 2001.

United States Government as presented by the Secretary of the Navy. Warfighting: MCDP-1 USMC PCN 142 000006 00. 20 March. 1997.

Wikipedia: The Free Encyclopedia. 15 April 2007. <http://www.wikipedia.org>.

Winters, Jackson H. “Smart Antenna Techniques and Their Application to Wireless Ad Hoc Networks.” Eigent Technologies, LLC IEEE Wireless Communications August. 2006.

Wullems, Chris; Tham, Kevin; Smith, Jason; and Looi, Mark. “A Trivial Denial of Service attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANS.” Information Security Research Centre; IEEE. 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Air Force Institute of Technology (AFIT)
   Wright Patterson AFB, OH

4. Air Force Communications Agency (AFCA)
   Scott AFB, IL

5. Alberto Hernandez
   DoD Biometrics Fusion Center
   Clarksburg, WV

6. Dr. Todd C. Marek, VP
   Communications, Networks & Electronics
   Atlanta, GA

7. Richard White, GS-15
   Air Force Information Warfare Center (AFIWC)
   Lackland AFB, TX

8. Dr. Dan Boger
   Chairman, Department of Information Sciences
   Naval Postgraduate School
   Monterey, CA